SmartGuard 600-Steuerungen

Benutzerhandbuch

Bestellnummern 1752-L24BBB, 1752-L24BBBE

ALLEN-BRADLEY • ROCKWELL SOFTWARE Rockwell Automation

Wichtige Hinweise für den Anwender

Die Betriebseigenschaften elektronischer Geräte unterscheiden sich von denen elektromechanischer Geräte. In der Publikation SGI-1.1, „Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls“ (erhältlich bei Ihrem Rockwell Automation-Vertriebsbüro oder online unter http://literature.rockwellautomation.com), werden einige wichtige Unterschiede zwischen elektronischen und fest verdrahteten elektromechanischen Geräten erläutert. Aufgrund dieser Unterschiede und der vielfältigen Einsatzbereiche elektronischer Geräte müssen die für die Anwendung dieser Geräte verantwortlichen Personen sicherstellen, dass die Geräte zweckgemäß eingesetzt werden.

Rockwell Automation ist in keinem Fall verantwortlich oder haftbar für indirekte Schäden oder Folgeschäden, die durch den Einsatz oder die Anwendung dieses Geräts entstehen.

Die in diesem Handbuch aufgeführten Beispiele und Abbildungen dienen ausschließlich zur Veranschaulichung. Aufgrund der unterschiedlichen Anforderungen der jeweiligen Anwendung kann Rockwell Automation keine Verantwortung oder Haftung für den tatsächlichen Einsatz der Produkte auf der Grundlage dieser Beispiele und Abbildungen übernehmen.

Rockwell Automation übernimmt keine patentrechtliche Haftung in Bezug auf die Verwendung von Informationen, Schaltkreisen, Geräten oder Software, die in dieser Publikation beschrieben werden.

Die Vervielfältigung des Inhalts dieser Publikation, ganz oder auszugsweise, bedarf der schriftlichen Genehmigung von Rockwell Automation.

In dieser Publikation werden folgende Hinweise verwendet, um Sie auf bestimmte Sicherheitsaspekte aufmerksam zu machen:

WARNUNG	Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die in explosionsgefährdeten Umgebungen zu einer Explosion und damit zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können.
WICHTIG	Dieser Hinweis enthält Informationen, die für den erfolgreichen Einsatz und das Verstehen des Produkts besonders wichtig sind.
ACHTUNG	Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. Achtungshinweise helfen Ihnen, eine Gefahr zu erkennen, die Gefahr zu vermeiden und die Folgen abzuschätzen.
STROMSCHLAG-GEFAHR	An der Außenseite oder im Inneren des Geräts (z. B. eines Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie darauf hinweist, dass möglicherweise eine gefährliche Spannung anliegt.
VERBRENNUNGS-GEFAHR	An der Außenseite oder im Inneren des Geräts (z. B. eines Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie darauf hinweist, dass die Oberflächen möglicherweise gefährliche Temperaturen aufweisen.

Allen-Bradley, Rockwell Automation, SmartGuard, Logix, ControlLogix, Guard I/O, POINT I/O, RSLogix 5000, RSNetWorx for DeviceNet, RSLinx und TechConnect sind Marken von Rockwell Automation, Inc.

Nicht Rockwell Automation zugehörige Marken sind das Eigentum der jeweiligen Unternehmen.

Im Folgenden sind die Änderungen in diesem Handbuch seit der letzten Drucklegung zusammengefasst.

Thema	Seite
Neue Informationen zur Steuerung 1752-L24BBBE	Im gesamten Handbuch
Neue Informationen zur Ethernet-Kommunikation	28
Neue Informationen zur Erdung der Steuerung 1752-L24BBBE	30
Aktualisierte Abbildung zur Verbindung des DeviceNet-Anschlusses	32
Neue Informationen zum Herstellen einer Verbindung zum Ethernet-Anschluss	33
Aktualisiertes Beispiel für die Not-Aus-Verdrahtung	38, 293
Aktualisiertes Beispiel für die Verdrahtung der Schutztür	38, 295
Neues Kapitel zum Einrichten Ihres EtherNet/IP-Netzwerks	Kapitel 4
Aktualisierte Informationen zur DeviceNet-Kommunikation	Kapitel 7
Neues Kapitel zum Konfigurieren Ihrer Steuerung für die EtherNet/IP-Kommunikation	Kapitel 8
Neue Tabelle mit EtherNet/IP-Fehlermeldungen	191
Aktualisierte Steuerungsspezifikationen	201
Aktualisierte Tabellen zu den Modulstatusanzeigen	207
Neue Informationen zum Erkennen von EtherNet/IP-Fehlern	218
Aktualisiertes Beispiel für die Zwei-Zonen-Verdrahtung	296
Aktualisiertes Beispiel für die Verdrahtung der Schaltmatte	298

Notizen:

Vorwort

An wen richtet sich dieses Handbuch? 13
Zweck dieses Handbuchs. 13
Zusätzliche Hilfsmittel 13
Allgemeine Verfahren, die in diesem Handbuch verwendet werden . . . 14

Kapitel 1

Überblick

Einleitung 15
Informationen zur SmartGuard 600-Steuerung 15
Hardware 17
Kommunikation. 20
Konfiguration und Programmierung 20
Status- und Fehlerüberwachung. 20
Sicherheitskonzept der Steuerung. 21
Zusätzliche Hilfsmittel 21

Kapitel 2

Installieren und Verdrahten der SmartGuard 600-Steuerung

Einleitung 23
Allgemeine Sicherheitsinformationen 23
Die Netzknotenadressierung 26
Festlegen der Netzknotenadresse 26
Festlegen der Kommunikationsgeschwindigkeit. 27
DeviceNet-Kommunikation. 27
Ethernet-Kommunikation. 28
Montage der SmartGuard-Steuerung. 29
Erden der SmartGuard-Steuerung 30
Anschließen der Stromversorgung 30
Herstellen von Kommunikationsverbindungen 31
Anschließen an den DeviceNet-Anschluss 32
Verbinden mit dem USB-Anschluss 33
Verbinden mit dem DeviceNet-Anschluss 33
Verdrahten der SmartGuard 600-Steuerung 34
Verdrahten von Eingangsgeräten 35
Verdrahten von Ausgangsgeräten 37
Verdrahtungsbeispiele. 38

Kapitel 3

Einrichten Ihres DeviceNet-Netzwerks

Einleitung 41
Anschließen eines Computers an das DeviceNet-Netzwerk 41
Konfigurieren des Treibers für das Netzwerk. 42
Stellen Sie sicher, dass der Treiber funktioniert 42
Inbetriebnahme aller Netzknoten. 42
Durchsuchen des Netzwerks 44
Konfigurationssignatur 45
Sicherheits-Reset (optional) 46
Festlegen von Kennwörtern (optional) 47
Festlegen oder Ändern von Kennwörtern 47
Vergessene Kennwörter 48

Kapitel 4

Einrichten Ihres EtherNet/IP-Netzwerks

Einleitung ... 51
Anschließen eines Computers an das EtherNet/IP-Netzwerk ... 51
Konfigurieren des Treibers für das Netzwerk ... 52
Stellen Sie sicher, dass der Treiber funktioniert ... 52
Anschließen der Steuerung SmartGuard 600 an das EtherNet/IP-Netzwerk ... 53
Festlegen der IP-Adresse ... 53
Verwendung von BOOTP zum Festlegen der IP-Adresse ... 54
Verwendung des Rockwell BOOTP-Dienstprogramms ... 55
Verwendung der Software RSLinx zum Festlegen der IP-Adresse ... 57
Netzwerkübergreifendes Bridging ... 59
EtherNet/IP-Netzwerk zu einem DeviceNet-Netzwerk ... 60
USB-Anschluss zum EtherNet/IP-Netzwerk ... 62

Kapitel 5

Verwalten der Sicherheitsnetzwerknummer

Einleitung ... 63
Formate der Sicherheitsnetzwerknummern (SNN) ... 63
Zeitbasierte Sicherheitsnetzwerknummer (empfohlen) ... 64
Manuelle Sicherheitsnetzwerknummer (SNN) ... 64
Zuweisen der Sicherheitsnetzwerknummer (SNN) ... 65
Automatisch (zeitbasiert) ... 65
Manuell ... 65
Festlegen der Sicherheitsnetzwerknummer (SNN) in allen Sicherheitsnetzknoten ... 65
Abweichung der Sicherheitsnetzwerknummer (SNN) ... 67
Ändern der Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse ... 67

Kapitel 6

Konfigurieren der zentralen E/A

Einleitung ... 69
Konfigurieren der zentralen Sicherheitseingänge ... 69
Beispiel: Eingangskanal als Testimpuls vom Testausgang ... 73
Automatische Anpassung von Ein- und Ausschaltverzögerungszeiten ... 74
Konfigurieren der zentralen Testausgänge ... 74
Konfigurieren der zentralen Sicherheitsausgänge ... 76

Kapitel 7

Konfigurieren der Steuerung für die DeviceNet-Kommunikation

Einleitung ... 79
Konfigurieren der Steuerung als Sicherheits-Master ... 79
Konfigurieren von E/A-Zielen für CIP Safety im DeviceNet-Netzwerk ... 80
Konfigurieren von E/A-Sicherheitsverbindungen ... 83
Ändern einer E/A-Verbindung ... 86
Konfigurieren der Steuerung als Sicherheits-Slave ... 90
Erstellen von Sicherheits-Slave-E/A-Daten ... 90

Arbeiten mit dem generischen Sicherheitsprofil in RSLogix 5000 ... 94
Verriegelungslogik zwischen zwei SmartGuard-Steuerungen ... 96
Konfigurieren der Steuerung als DeviceNet-Standard-Slave ... 98
Erstellen von Standard-Slave-E/A-Daten ... 98
Hinzufügen des SmartGuard-Standard-Slaves zur Abtastliste des Standard-Masters ... 102
Lesen und Schreiben von der und auf die SmartGuard-Steuerung zu einer PanelView Plus-Schnittstelle ... 103
Lesen von BOOLs aus der SmartGuard-Steuerung und anschließendes Anzeigen der BOOLS auf der PanelView Plus-Schnittstelle ... 104
Konfigurieren der Abtastliste des PanelView-Scanners ... 106
Konfigurieren Sie den RN10C-DeviceNet-Scanner ... 107
Gleichzeitiges Lesen und Schreiben von der und auf die SmartGuard-Steuerung von der PanelView Plus-Schnittstelle aus ... 113
Konfigurieren der Abtastliste des PanelView-Scanners ... 116
Konfigurieren Sie den RN10C-DeviceNet-Scanner ... 118
Konfigurieren der Daten, die von der PanelView Plus-Schnittstelle auf die SmartGuard-Steuerung geschrieben werden ... 119
COS vs. abgefragt ... 123
Maximale Verbindungsgrößen ... 125

Kapitel 8

Konfigurieren Ihrer Steuerung für die EtherNet/IP-Kommunikation

Einleitung ... 129
Multicast-Verbindungen ... 129
Konfigurieren der Ziel-E/A in der Software RSNetWorx for DeviceNet ... 130
Konfigurieren Ihrer Steuerung als Slave mithilfe des generischen Profils der Software RSLogix 5000 ... 134
Konfigurieren der Kommunikation zwischen einem Standard-PanelView-Terminal und einer SmartGuard 600-Steuerung über ein EtherNet/IP-Netzwerk ... 136

Kapitel 9

Einrichten der Steuerungsmodi

Einleitung ... 139
Einrichten des automatischen Ausführungsmodus (optional) ... 139
Einrichten des eigenständigen Kommunikationsmodus (optional) ... 140
Ändern des Modus einer Steuerung ... 142

Kapitel 10

Erstellen eines Anwendungsprogramms

Einleitung ... 143
Der Logik-Editor ... 143
Grundlagen der Programmierung ... 144
Logische Funktionen und Funktionsblöcke ... 145
Eingangs-Tags ... 145
Ausgangs-Tags ... 147

E/A-Kommentarfunktion 148
Einschränkungen bei der Programmierung 148
Erstellen eines Funktionsblockprogramms 149
Hinzufügen eines Eingangs- oder Ausgangs-Tags 149
Hinzufügen eines Funktionsblocks 149
Verbinden der Tags mit dem Funktionsblock 150
Bearbeiten von Funktionsblockparametern 150
Ein-/Ausgangseinstellungen 151
Optionale Ausgangspunktauswahl 152
Kommentare 152
Suchen von Funktionsblöcken mit offenen Verbindungen 153
Programmieren auf mehreren Seiten 154
Speichern des Programms 155
Aktualisieren des Programms 155
Online-Überwachung des Programms 156
Abfolge der Programmausführung 157
Benutzerdefinierte Funktionsblöcke 158
Erstellen von benutzerdefinierten Funktionsblöcken 158
Schützen von benutzerdefinierten Funktionsblöcken durch ein Kennwort 160
Wiederverwenden der Dateien mit benutzerdefinierten Funktionsblöcken 161
Hinweise für das Wiederverwenden von benutzerdefinierten Funktionsblöcken 162
Zusätzliche Hilfsmittel 163

Kapitel 11

Herunterladen und Überprüfen

Einleitung 165
Herunterladen der DeviceNet-Netzwerkkonfiguration 165
Überprüfen der DeviceNet-Sicherheitskonfiguration 167
Starten des Assistenten zur Überprüfung von Sicherheitsgeräten 167
Ermitteln, ob Geräte überprüft werden können 168
Auswählen der zu prüfenden Geräte 169
Überprüfen der Prüfberichte für Sicherheitsgeräte 171
Verriegeln von Sicherheitsgeräten 172
Überprüfen der Zusammenfassung des Assistenten zur Überprüfung von Sicherheitsgeräten 173

Kapitel 12

Zustandsüberwachung und Fehlerbehebung

Einleitung 175
Statusanzeigen 175
Alphanumerische Anzeige 176
Überwachen des E/A-Stromversorgungseingangs 177
Überwachen der E/A-Wartungsinformationen 178
Kontaktbetriebszähler-Überwachung 178
Gesamtaktivzeit-Überwachung 178
Konfigurieren eines Wartungsüberwachungsmodus 179
Löschen der Wartungswerte 180
Anzeigen von E/A-Statusdaten 181

Allgemeine Statusdaten ... 182
Status zentraler Eingang ... 183
Status zentraler Ausgang ... 183
Status Testausgang oder Muting-Lampe ... 183
Steuerungsanschlussstatus (Sicherheits-Slave-Funktion) ... 184
Fehlerkategorien ... 187
Tabelle mit der Fehlerhistorie ... 188
Speicherbereich für die Fehlerhistorie ... 188
Anzeigen der Tabelle mit der Fehlerhistorie für die Steuerung 1752-L24BBB ... 188
Anzeigen der Tabelle mit der EtherNet/IP-Fehlerhistorie für die Steuerung 1752-L24BBBE ... 189
Tabelle mit Ethernet-Fehlerhistorie ... 190
Meldungen der Fehlerhistorie und erforderliche Maßnahmen ... 191
Download-Fehler und Abhilfemaßnahmen ... 196
Rücksetzfehler und Abhilfemaßnahmen ... 198
Modusänderungsfehler und Abhilfemaßnahmen ... 200

Anhang A

Steuerungsspezifikationen

Einleitung ... 201
Allgemeine Spezifikationen ... 201
Umgebungsspezifikationen ... 203
Zertifizierungen ... 205

Anhang B

Statusanzeigen

Einleitung ... 207
Modulstatusanzeigen ... 207
Fehleridentifikation mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige ... 213
Identifikation von EtherNet/IP-Fehlern mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige ... 218

Anhang C

Befehlsreferenz zu den Logikfunktionen

Einleitung ... 219
NOT-Befehl (Logisches Nicht) ... 219
Diagramm NOT-Befehl ... 219
Wahrheitstabelle für den NOT-Befehl ... 219
AND-Befehl (Logisches Und) ... 220
Diagramm AND-Befehl ... 220
Wahrheitstabelle für den AND-Befehl ... 220
OR-Befehl (Logisches Oder) ... 222
Diagramm OR-Befehl ... 222
Wahrheitstabelle für den OR-Befehl ... 222
Exclusive OR-Befehl (Exklusives Oder) ... 224
Diagramm Exclusive OR-Befehl ... 224
Wahrheitstabelle für den Exclusive OR-Befehl ... 225
Exclusive NOR-Befehl (Exklusives Nicht-Oder) ... 225
Diagramm Exclusive NOR-Befehl ... 225
Wahrheitstabelle für den Exclusive NOR-Befehl ... 225

Routing-Befehl 226
Diagramm Routing-Befehl 226
Wahrheitstabelle für den Routing-Befehl 226
RS-FF-Befehl (Reset Set Flip-flop) 226
Diagramm RS-FF-Befehl 226
Fehlerhandhabung beim Reset Set FIip-flop-Befehl 227
Zeitdiagramm für den RS-FF-Befehl. 227
Multi-connector-Befehl (Mehrere Anschlüsse) 227
Diagramm Multi-connector-Befehl 227
Wahrheitstabelle für den Multi-connector-Befehl 228
Comparator-Befehl (Vergleicher) 228
Diagramm Comparator-Befehl 229
Parameter des Comparator-Befehls. 229
Wahrheitstabelle für den Comparator-Befehl 230
Zeitdiagramm für den Comparator-Befehl 231

Anhang D

Befehlsreferenz zu den Funktionsblöcken

Einleitung 233
Funktionsblock Reset (Zurücksetzen) 233
Parameter des Funktionsblocks Reset. 234
Zeitdiagramme für den Funktionsblock Reset 235
Funktionsblock „Restart“ (Neustart) 235
Parameter des Funktionsblocks Restart 236
Zeitdiagramme für den Funktionsblock „Restart“ (Neustart) 237
Not-Aus (ESTOP) 237
Parameter des Funktionsblocks „ESTOP“ 238
Wahrheitstabelle für den Funktionsblock „ESTOP“ 239
Fehlerbehandlung für den Funktionsblock „ESTOP“ 239
Zeitdiagramm für den Funktionsblock „ESTOP“. 240
Funktionsblock „Light Curtain“ (Lichtgitter) (LC) 240
Parameter des Funktionsblocks „Light Curtain“ (Lichtgitter) . . . 241
Wahrheitstabellen für den Funktionsblock „Light Curtain“ (Lichtgitter). 241
Fehlerbehandlung für den Funktionsblock „Light Curtain“ (Lichtgitter). 241
Zeitdiagramm für den Funktionsblock „Light Curtain“ (Lichtgitter). 242
Funktionsblock „Safety Gate Monitoring“ (Sicherheitstürüberwachung). 242
Optionale Ausgänge für den Funktionsblock „Safety Gate Monitoring“ (Sicherheitstürüberwachung) 243
Einstellung des Ausgangs „Fault Present“ für den Funktionsblock „Safety Gate Monitoring“ 243
Funktionstests für den Funktionsblock „Safety Gate Monitoring“ 243
Parameter des Funktionsblocks „Safety Gate Monitoring“. 244
Wahrheitstabellen für den Funktionsblock „Safety Gate Monitoring“ 245

Fehlerbehandlung für den Funktionsblock „Safety Gate Monitoring“ ... 245
Zeitdiagramme für den Funktionsblock „Safety Gate Monitoring“ ... 246
Funktionsblock Two-hand Control (2-Hand-Betätigung) ... 247
Optionale Ausgänge für den Funktionsblock Two-hand Control ... 248
Einstellung des Ausgangs „Fault Present“ für den Funktionsblock Two-hand Control ... 248
Parameter des Funktionsblocks Two-hand Control ... 248
Wahrheitstabelle für den Funktionsblock Two-hand Control ... 249
Fehlerbehandlung für den Funktionsblock Two-hand Control ... 250
Zeitdiagramm für den Funktionsblock Two-hand Control ... 250
Funktionsblock OFF-delay Timer (Ausschaltverzögerter Timer) ... 251
Zeitdiagramm für den Funktionsblock OFF-delay Timer ... 251
Funktionsblock „ON-delay Timer“ (Einschaltverzögerter Timer) ... 251
Zeitdiagramm für den Funktionsblock ON-delay Timer ... 252
Funktionsblock „User Mode Switch“ (Anwendermodus-Schalter) ... 252
Optionale Ausgänge für den Funktionsblock User Mode Switch ... 252
Einstellung des Ausgangs „Fault Present“ für den Funktionsblock User Mode Switch ... 253
Wahrheitstabelle für den Funktionsblock User Mode Switch ... 253
Fehlerbehandlung für den Funktionsblock User Mode Switch ... 253
Zeitdiagramm für den Funktionsblock User Mode Switch ... 254
External Device Monitoring (EDM, Externe Geräteüberwachung) ... 254
Optionale Ausgänge für den EDM-Funktionsblock ... 255
Einstellung des Ausgangs „Fault Present“ für den EDM-Funktionsblock ... 255
Parameter des EDM-Funktionsblocks ... 255
Fehlerbehandlung für den EDM-Funktionsblock ... 255
Zeitdiagramm für den EDM-Funktionsblock ... 256
Muting ... 256
Parameter des Funktionsblocks Muting ... 257
Optionale Ausgänge für den Funktionsblock Muting ... 258
Einstellung des Ausgangs „Fault Present“ für den Funktionsblock Muting ... 258
Fehlerbehandlung für den Funktionsblock Muting ... 258
Detailbeschreibung der Muting-Funktion ... 259
Beispiel: Paralleles Muting mit 2 Sensoren ... 260
Beispiel: Positionserfassung ... 268
Beispiel: Überbrückungsfunktion ... 270
Enable Switch (Zustimmschalter) ... 273
Parameter des Funktionsblocks Enable Switch ... 274
Optionale Ausgänge ... 274
Einstellung des Ausgangs „Fault Present“ ... 274
Fehlerbehandlung für den Funktionsblock Enable Switch ... 275
Zeitdiagramme für den Funktionsblock Enable Switch ... 275
Pulse Generator (Impulsgenerator) ... 276

Parameter des Funktionsblocks Pulse Generator. 276
Zeitdiagramm für den Funktionsblock Pulse Generator 277
Counter (Zähler) 277
Parameter des Funktionsblocks Counter. 277
Rücksetzbedingung 278
Zähltyp 278
Zeitdiagramme für den Funktionsblock Counter 278

Anhang E

Explizite Nachrichten

Einleitung 281
Empfangen expliziter Nachrichten 281
Befehlsformat 281
Antwortformat 282
Fehlerantwortformat. 283
Beispiel für eine Lesenachricht einer GuardLogix-Steuerung. 284
Senden expliziter Nachrichten 284
Einschränkungen beim Senden expliziter Nachrichten 285
Zugriff auf Steuerungsparameter mit expliziten DeviceNet-Nachrichten 286

Anhang F

Anwendungs- und Konfigurationsbeispiele

Einleitung 293
Not-Aus-Anwendung. 293
Sicherheitstüranwendung mit automatischer Rücksetzung 295
Zwei-Zonen-Sicherheitstüranwendung unter Verwendung eines Not-Aus-Schalters mit manueller Rücksetzung. 296
Sicherheitsmattenanwendung 298
Lichtgitteranwendung 300

Glossar

Index

Lesen Sie dieses Vorwort, um sich mit dem Handbuch vertraut zu machen. Es enthält Informationen über:

- das Zielpublikum dieses Handbuchs.
- den Zweck dieses Handbuchs.
- zusätzliche Hilfsmittel.
- im Handbuch verwendete Konventionen.

An wen richtet sich dieses Handbuch?

Verwenden Sie dieses Handbuch, wenn Sie für die Entwicklung, Installation, Programmierung oder Entstörung von Steuerungssystemen verantwortlich sind, in denen SmartGuard 600-Steuerungen verwendet werden.

Sie müssen ein grundlegendes Verständnis von elektrischen Schaltungen haben und sich mit Relaislogik auskennen. Sie müssen außerdem ausgebildet und erfahren in der Erstellung, dem Betrieb und der Wartung von Sicherheitssystemen sein.

Zweck dieses Handbuchs

Bei diesem Handbuch handelt es sich um eine Anleitung für die Verwendung von SmartGuard 600-Steuerungen. Dabei werden die jeweiligen Verfahren für die Konfiguration, den Betrieb und die Entstörung Ihrer SmartGuard 600-Steuerung beschrieben.

Zusätzliche Hilfsmittel

In der folgenden Tabelle finden Sie eine Liste von Publikationen, die wichtige Informationen zu SmartGuard 600-Steuerungssystemen enthalten.

Hilfsmittel	Beschreibung
Steuerung SmartGuard 600 – Installationsanleitung, Publikation 1752-IN001	Informationen zur Installation der Steuerung SmartGuard 600
SmartGuard 600-Steuerungen – Sicherheitsreferenzhandbuch, Publikation 1752-RM001	Ausführliche Anforderungen für das Erreichen und Beibehalten von SIL 3 mit dem SmartGuard-Steuerungssystem
CompactBlock Safety E/A-Module für DeviceNet Serie 1791DS – Installationsanleitung, Publikation 1791DS-IN001	Informationen zur Installation von Guard I/O DeviceNet Safety-Modulen
Guard I/O DeviceNet Safety Modules User Manual, Publikation 1791DS-UM001	Informationen zur Verwendung von Guard I/O DeviceNet Safety-Modulen
DeviceNet Media Design Installation Guide, Publikation DNET-UM072	Informationen zur Planung Ihres EtherNet/IP-Netzwerks

Sie können die Publikationen unter http://literature.rockwellautomation.com ansehen oder herunterladen. Wenn Sie gedruckte Exemplare technischer Dokumente bestellen möchten, wenden Sie sich an Ihren Distributor oder Vertriebsbeauftragten von Rockwell Automation.

Allgemeine Verfahren, die in diesem Handbuch verwendet werden

In diesem Handbuch gelten folgende Konventionen:

- Listen mit Gliederungspunkten (wie die vorliegende) stellen Informationen bereit, nicht aber Verfahrensschritte.
- Nummerierte Listen enthalten aufeinander folgende Schritte oder hierarchische Informationen.

Überblick

Einleitung

Thema	Seite
Informationen zur SmartGuard 600-Steuerung	15
Sicherheitskonzept der Steuerung	21
Zusätzliche Hilfsmittel	21

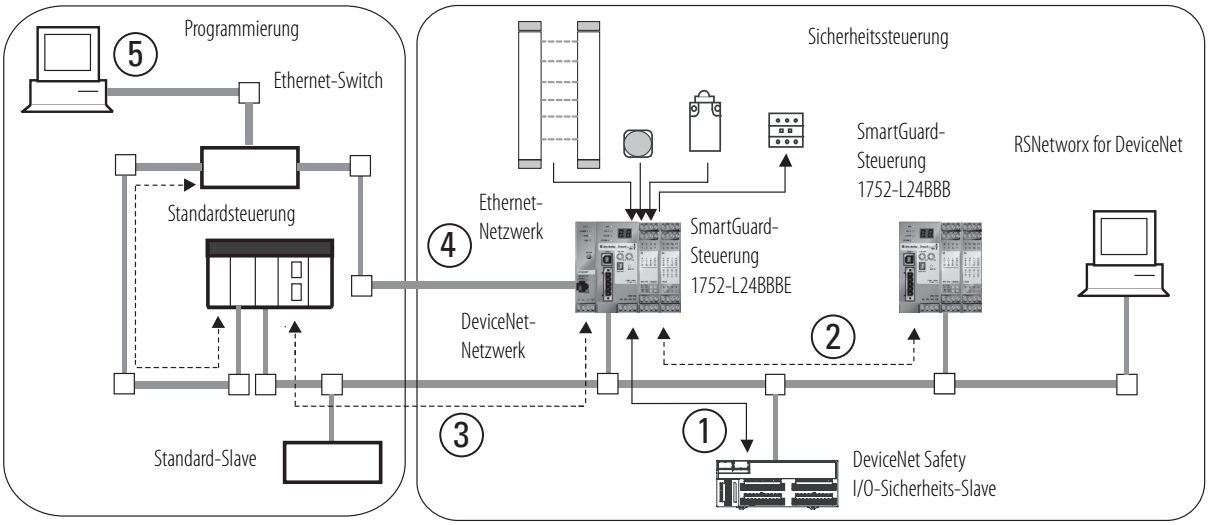
Informationen zur SmartGuard 600-Steuerung

Die Steuerungen SmartGuard 600 (Bestellnummer 1752-L24BBB und 1752-L24BBBE) ist ein programmierbares elektronisches System mit 16 Digitaleingängen, 8 Digitalausgängen, 4 Testimpulsquellen und Anschlüssen für USB- und DeviceNet-Kommunikation. Außerdem verfügt die Steuerung 1752-L24BBBE über EtherNet/IP-Konnektivität.

Die Steuerung SmartGuard 600 unterstützt Standard- und CIP Safety-Kommunikation über DeviceNet-Netzwerke sowie Standard-CIP-Kommunikation über EtherNet/IP-Netzwerke.

Die Steuerung SmartGuard 600 ist für die Verwendung in Sicherheitsanwendungen bis einschließlich SIL 3 (Safety Integrity Level) gemäß IEC 61508, für PL(e) gemäß ISO 13849-1 und Kategorie (CAT) 4 gemäß EN 954-1 zertifiziert.

Beispiel für ein Sicherheitssteuerungssystem mit SmartGuard 600-Steuerung

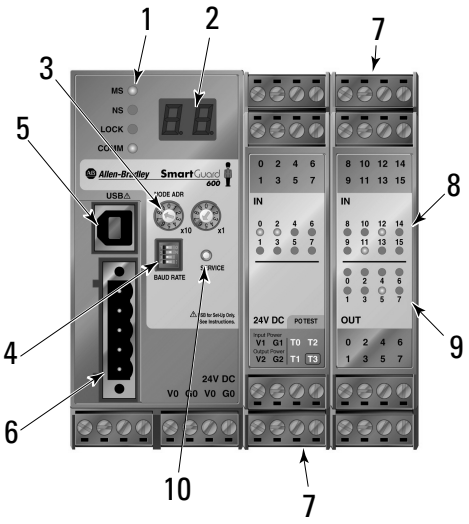


Nummer	Beschreibung
1	Als DeviceNet-Sicherheits-Master kann die Steuerung SmartGuard 600 bis zu 32 Guard I/O-Module steuern. Diese 1791DS- und 1732DS-Module sind dieselben dezentralen Sicherheits-E/A-Module, die mit GuardLogix-Steuerungen verwendet werden.
2	Als DeviceNet-Sicherheits-Slave verhält sich die Steuerung SmartGuard 600 aus der Perspektive eines Sicherheits-Masters wie dezentrale Sicherheits-E/A. Ein GuardLogix- oder ein anderer SmartGuard-Sicherheits-Master kann Sicherheitsdaten von der SmartGuard-Slave-Steuerung lesen und auf diese schreiben. Auf diese Weise kann die dezentrale Sicherheitssteuerung durch Sperrung mehrerer Steuerungen über CIP Safety auf DeviceNet-Netzwerken erfolgen.
3	Als DeviceNet-Standard-Slave kann die Steuerung SmartGuard 600 die Funktion eines dezentralen Standard-E/A-Moduls übernehmen und auf explizite Nachrichten antworten, sodass Standard-DeviceNet-Master wie ControlLogix-, SLC 500- oder PLC-5-Steuerungen oder eine Bedieneinheit Daten von der Steuerung SmartGuard 600 lesen und auf diese schreiben können. Dies erleichtert die Koordination mit Ihrer Standard-SPS-Anwendung, die unter anderem die Anzeige von Informationen zum Sicherheitssystem auf einer Bedieneinheit umfasst.
4	Als EtherNet/IP-Standardziel kommuniziert die Steuerung SmartGuard 600 mit einem Ethernet/IP-Standard-Master wie eine CompactLogix- oder MicroLogix-Steuerung oder ein HMI-Gerät. Die SmartGuard-Steuerung unterstützt CIP Safety bei der EtherNet/IP-Kommunikation nicht. Daher kann die SmartGuard-Steuerung keine 1791ES-Sicherheitsmodule steuern. Die gesamte Sicherheitssteuerung muss über das DeviceNet-Netzwerk erfolgen wie oben unter den Nummern 1 und 2 dargestellt.
5	Als eingeschränktes EtherNet/IP-Überbrückungsgerät ermöglicht die Steuerung SmartGuard 600 die Überbrückung zu DeviceNet durch Programmier-Tools, um die Steuerung SmartGuard 600 anzeigen und programmieren und andere DeviceNet-Geräte konfigurieren zu können.

Hardware

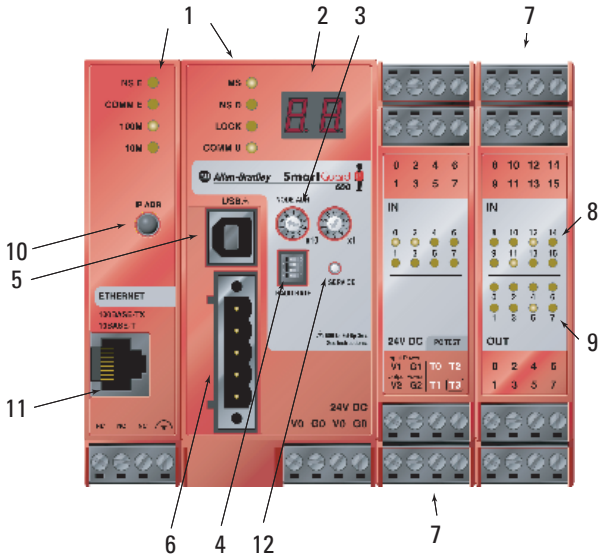
Die Steuerung SmartGuard 600 (Bestellnummer 1752-L24BBB und 1752-L24BBBE) bieten 16 Digitaleingänge, 8 Digitalausgänge, 4 Impulstestquellen und Verbindungen über das USB- und DeviceNet-Sicherheitsprotokoll. Außerdem verfügt die Steuerung 1752-L24BBBE über EtherNet/IP-Konnektivität.

Steuerung SmartGuard 600 (Bestellnummer 1752-L24BBB) – Leistungsmerkmale



Nummer	Leistungsmerkmal
1	Modulstatusanzeigen
2	Alphanumerische Anzeige
3	Netzknotenadressschalter
4	Baudratenschalter
5	USB-Anschluss
6	DeviceNet-Kommunikationsanschluss
7	Klemmenanschlüsse
8	Eingangsstatusanzeigen
9	Ausgangsstatusanzeigen
10	Service-Schalter

Steuerung SmartGuard 600 (Bestellnummer 1752-L24BBBE) – Leistungsmerkmale



Nummer	Leistungsmerkmal
1	Modulstatusanzeigen
2	Alphanumerische Anzeige
3	Netzknotenadressschalter
4	Baudratenschalter
5	USB-Anschluss
6	DeviceNet-Kommunikationsanschluss
7	Klemmenanschlüsse
8	Eingangsstatusanzeigen
9	Ausgangsstatusanzeigen
10	Schalter für die Anzeige der IP-Adresse
11	Ethernet-Anschluss
12	Service-Schalter

Sicherheitseingänge

Die Steuerung verfügt über 16 zentrale Sicherheitseingänge, die die folgenden Funktionen unterstützen.

- Eingangsschaltungsdiagnose – Mit Testimpulsquellen können interne Schaltungen, externe Geräte und externe Anschlüsse überwacht werden.
- Ein- und Ausschaltverzögerung des Eingangs – Sie können Eingangszeitfilter zwischen 0 und 126 ms in Vielfachen der Steuerungszykluszeit eingeben. Wenn Sie für den Eingang Ein- und Ausschaltverzögerungen festlegen, können die Auswirkungen von Rattern und externem Rauschen verringert werden.
- Zweikanalmodus – Für Paare zusammengehöriger zentraler Eingänge können Sie den Zweikanalmodus festlegen. Wenn der Zweikanalmodus eingestellt ist, können Zeitabweichungen in den Datenänderungen oder Eingangssignalen zwischen zwei gepaarten zentralen Eingängen ausgewertet werden.

Sicherheitsausgänge

Die Steuerung verfügt über acht zentrale Sicherheitsausgänge, die die folgenden Funktionen unterstützen.

- Ausgangsschaltungsdiagnose – Mit Testimpulsen können interne Schaltungen, externe Geräte und externe Anschlüsse der Steuerung diagnostiziert werden.
- Überstromerkennung und -schutz – Zum Schutz des Stromkreises wird ein Ausgang blockiert, sobald ein Überstrom erkannt wird.
- Zweikanalmodus – Beide Ausgänge des Paares können auf einen Sicherheitsstatus festgelegt werden, wenn ohne Einfluss des Anwenderprogramms an einem der paarweisen zentralen Ausgänge ein Fehler auftritt.

Testimpulsquellen

Vier voneinander unabhängige Testausgänge werden normalerweise zusammen mit den Sicherheitseingängen verwendet. Sie können auch für die Verwendung als Ausgangsklemmen für das Standardsignal konfiguriert werden. Die Testimpulsausgänge unterstützen die folgenden Funktionen.

- Überstromerkennung und -schutz – Zum Schutz des Stromkreises wird ein Ausgang blockiert, sobald ein Überstrom erkannt wird.
- Stromstärkeüberwachung für Muting-Lampe – Trennungen können nur an Klemme T3 erkannt werden.

Kommunikation

Die Steuerung kann als DeviceNet-Sicherheits-Master oder -Slave, als DeviceNet-Standard-Slave oder als eigenständige Steuerung eingesetzt werden, wenn die DeviceNet-Kommunikation deaktiviert ist. Eine einzelne Steuerung kann gleichzeitig als Sicherheits-Master, als Sicherheits-Slave und als Standard-Slave eingesetzt werden.

Mit expliziten Nachrichten können Statusinformationen über die Steuerung gelesen werden. Das Anwenderprogramm kann so konfiguriert werden, dass es explizite Nachrichten vom Anwenderprogramm aus sendet. Ein Routing der Nachrichten zwischen DeviceNet- und EtherNet/IP-Netzwerk ist möglich.

Der USB-Anschluss kann für das Programmieren der SmartGuard-Steuerung verwendet werden und zum Konfigurieren von Geräten im DeviceNet-Netzwerk. SmartGuard bietet einige beschränkte Pass-Through-Funktionen von USB zu DeviceNet, die für das Programmieren und die Konfiguration verwendet werden können. Bei der Verwendung im eigenständigen Modus kommuniziert die Steuerung über USB mit der Konfigurationssoftware.

Konfiguration und Programmierung

Verwenden Sie die Software RSNetWorx for DeviceNet, Version 8.0 (mindestens) oder höher (Version 9.1 wird empfohlen), für die Konfiguration und Programmierung der Steuerung 1752-L24BBB sowie zur Überwachung ihres Status. Mithilfe der Software RSNetWorx for DeviceNet, Version 9.1 oder höher, können Sie die Steuerung 1752-L24BBBE konfigurieren. RSNetWorx for DeviceNet ermöglicht das Konfigurieren der Steuerung über den USB-Anschluss der SmartGuard-Steuerung oder über das DeviceNet- oder EtherNet/IP-Netzwerk.

Außerdem benötigen Sie die Software RSLinx, Version 2.55 oder höher, mit der Sie die Steuerung 1752-L24BBBE über EtherNet/IP konfigurieren können.

Der Logic Editor wird von RSNetWorx for DeviceNet gestartet. Es werden sowohl grundlegende logische Funktionen wie AND und OR als auch Funktionsblöcke wie ESTOP und Lichtgitter unterstützt. Es können maximal 254 logische Funktionen und Funktionsblöcke auf höchstens 32 Programmierseiten verwendet werden. Sie können sowohl die Konfigurationsdaten als auch die Projektdateien mit einem Kennwort schützen.

Status- und Fehlerüberwachung

Die internen Statusinformationen der Steuerung sowie die E/A-Daten können online mit RSNetWorx for DeviceNet über eine USB-, DeviceNet- oder EtherNet/IP-Netzwerkverbindung überwacht werden.

Die Statusanzeigen und die alphanumerische Anzeige an der Steuerung geben Status- und Fehlerinformationen an. Wenn der Service-Schalter an der Vorderseite der Steuerung gedrückt wird, zeigt die alphanumerische Anzeige die Sicherheitskonfigurationssignatur an, wobei jeweils zwei Stellen und insgesamt zehn Zahlenpaare angezeigt werden.

Wenn der Schalter für die Anzeige der IP-Adresse mindestens 1 Sekunde lang gedrückt wird, erscheint in der Anzeige die festgelegte EtherNet/IP-Adresse.

Von der Steuerung erkannte Fehler werden in einem Fehlerverlaufsprotokoll und in einem EtherNet/IP-Verlaufsprotokoll erfasst. Dabei wird auch die Zeit aufgezeichnet, zu der der Fehler aufgetreten ist. (Die angezeigte Zeit wird als Gesamtbetriebszeit seit dem Einschalten der Steuerung angezeigt.)

Sicherheitskonzept der Steuerung

Die Steuerung SmartGuard 600 ist für die Verwendung in Sicherheitsanwendungen bis einschließlich SIL 3 (Safety Integrity Level) gemäß IEC 61508, für PL(e) gemäß ISO 13849-1 und Kategorie (CAT) 4 gemäß EN 954-1 zertifiziert (in dieser Norm entspricht der ausgeschaltete Zustand dem Sicherheitszustand). Zu den Anforderungen für Sicherheitsanwendungen gehört das Einschätzen der Wahrscheinlichkeit von Ausfallraten (PFD und PFH), Berechnungen der Systemreaktionszeit und funktionale Überprüfungen nach den SIL-3-Kriterien. Sie sollten diese Anforderungen lesen, verstehen und umsetzen, bevor Sie ein auf einer SmartGuard 600-Steuerung basierendes SIL-3- oder CAT-4-Sicherheitssystem in Betrieb nehmen.

Die Steuerung verwendet folgende Verfahren zur Unterstützung der Integrität von Sicherheitsdaten.

- SNN (Safety network number) – Eine eindeutige Nummer, die das Sicherheitsnetzwerk kennzeichnet. CIP Safety-Netzknoten müssen über eine eindeutige SNN- und DeviceNet-Netzwerkadresse verfügen.
- Konfigurationssignatur – Die Kombination aus ID-Nummer, Datum und Uhrzeit, die eine bestimmte Konfiguration für ein Sicherheitsgerät eindeutig kennzeichnet.
- Konfigurationssperre (oder Sicherheitsverriegelung) – Nachdem die Konfigurationsdaten heruntergeladen und überprüft wurden, können Sie die Konfiguration der Steuerung sperren, um Änderungen zu verhindern.
- Kennwortschutz – Sie können die Konfiguration der Steuerung durch ein optionales Kennwort schützen. Wenn Sie ein Kennwort festlegen, ist dieses für das Herunterladen, Sperren, Entsperren, Zurücksetzen und Ändern des Status der Steuerung erforderlich.

Sie müssen eine eindeutige, logische und sichtbare Unterscheidung zwischen den Sicherheits- und Standardteilen der Anwendung erstellen und dokumentieren.

Zusätzliche Hilfsmittel

Weitere Informationen über die Anforderungen für SIL-3- und CAT-4-Sicherheitssysteme, einschließlich der Intervalle für funktionale Überprüfungen, Systemreaktionszeit und PFD-/PFH-Werte, finden Sie im Sicherheitsreferenzhandbuch für die SmartGuard-Steuerungen, Publikation 1752-RM001.

Notizen:

Installieren und Verdrahten der SmartGuard 600-Steuerung

Einleitung

Thema	Seite
Allgemeine Sicherheitsinformationen	23
Die Netzknotenadressierung	26
Festlegen der Netzknotenadresse	26
Festlegen der Kommunikationsgeschwindigkeit	27
Montage der SmartGuard-Steuerung	29
Erden der SmartGuard-Steuerung	30
Anschließen der Stromversorgung	30
Verdrahten der SmartGuard 600-Steuerung	34

Allgemeine Sicherheitsinformationen

ACHTUNG

Umgebung und Gehäuse

Dieses Gerät ist für den Einsatz in industriellen Umgebungen des Verschmutzungsgrads 2, in Anwendungen der Überspannungskategorie II (gemäß Definition in IEC-Publikation 60664-1) bei Höhen bis zu 2000 m ohne Leistungsminderung bestimmt.

Gemäß IEC/CISPR-Publikation 11 entspricht dieses Produkt einem industriellen Gerät der Gruppe 1, Klasse A. Bei Nichtbeachtung der entsprechenden Vorsichtsmaßnahmen kann die elektromagnetische Verträglichkeit in anderen Umgebungen aufgrund von leitungsgeführten und abgestrahlten Störungen eventuell nicht gewährleistet werden.

Dieses Gerät wird in „offener" Ausführung geliefert. Es muss in ein Gehäuse eingebaut werden, das für diese speziellen Umgebungsbedingungen zugelassen ist und den Zugriff auf leitfähige Teile und damit das Risiko von Verletzungen verhindert. Das Gehäuse muss über ausreichende flammwidrige Eigenschaften verfügen, um die Ausbreitung von Flammen (gemäß Flammenausbreitungsklassifizierung oder 5VA, V2, V1, V0 bzw. einer ähnlichen Klassifizierung) zu verhindern oder zu minimieren, wenn es sich um ein nicht metallisches Gehäuse handelt. Das Innere des Gehäuses darf nur unter Zuhilfenahme eines Werkzeugs zugänglich sein. Nachfolgende Abschnitte dieser Publikation können zusätzliche Informationen bezüglich der spezifischen Gehäuseschutzklassen enthalten, die erforderlich sind, um bestimmte Produktsicherheits-Zertifizierungen einzuhalten.

Ergänzende Informationen zu dieser Publikation finden Sie in folgenden Dokumenten:

- Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Allen-Bradley-Publikation 1770-4.1.
- Die NEMA-Publikation 250 zu den geltenden Standards sowie die IEC-Publikation 60529 enthalten Erklärungen zu den Schutzgraden, die durch die verschiedenen Gerätetypen gewährleistet werden.

Zulassung für explosionsgefährdete Standorte – Nordamerika

The following information applies when operating this equipment in hazardous locations	**Informations sur l'utilisation de cet équipement en environnements dangereux**
Products marked CL I, DIV 2, GP A, B, C, D are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest T number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués CL I, DIV 2, GP A, B, C, D ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING **EXPLOSION HAZARD** • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**AVERTISSEMENT** **RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Folgende Informationen gelten beim Betrieb dieses Geräts an explosionsgefährdeten Standorten

Produkte mit der Kennzeichnung CL I, DIV 2, GP A, B, C, D sind nur für die Verwendung an explosionsgefährdeten Standorten der Klasse I, Division 2, Gruppen A, B, C, D sowie an nicht explosionsgefährdeten Standorten zugelassen. Bei allen Produkten ist auf dem Typenschild der Temperaturcode für den explosionsgefährdeten Standort angegeben. Bei der Kombination von Produkten innerhalb eines Systems sollte der allgemeine Temperaturcode des Systems anhand des niedrigsten Temperaturcodes (kleinste T-Zahl) bestimmt werden. Kombinationen der Geräte in Ihrem System müssen bei der Installation durch die örtliche, zuständige Behörde überprüft werden.

WARNUNG

EXPLOSIONSGEFAHR

- Geräte dürfen erst dann vom System getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt.
- Verbindungen zu den Geräten dürfen erst dann getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt. Sichern Sie alle externen Verbindungen zu diesen Geräten durch Schrauben, Schieberiegel, Gewindesteckverbinder oder andere geeignete, mit diesem Produkt zur Verfügung gestellte Befestigungselemente.
- Ein Austausch von Komponenten kann die Eignung für Klasse I, Division 2 beeinträchtigen.
- Wenn das Produkt Batterien enthält, dürfen diese nur an einem bekanntermaßen nicht explosionsgefährdeten Bereich gewechselt werden.

ACHTUNG

Programmierbares elektronisches Sicherheitssystem (PES)

Das für die Anwendung sicherheitsrelevanter programmierbarer elektronischer Systeme (PES) verantwortliche Personal muss die Sicherheitsanforderungen der Anwendung des Systems kennen und in der Verwendung des Systems geschult sein.

ACHTUNG

Verhindern elektrostatischer Entladungen

Dieses Gerät ist empfindlich gegen elektrostatische Entladungen, die zu internen Beschädigungen führen und den ordnungsgemäßen Betrieb beeinträchtigen können. Befolgen Sie folgende Richtlinien beim Umgang mit dem Gerät.

- Berühren Sie einen geerdeten Gegenstand, um eventuelle elektrische Ladung abzuleiten.
- Tragen Sie ein zugelassenes Erdungsarmband.
- Berühren Sie keine Verbinder oder Stifte an den Platinen der Komponenten.
- Berühren Sie keine Schaltkreiskomponenten im Gerät.
- Verwenden Sie möglichst einen vor statischen Entladungen sicheren Arbeitsplatz.
- Bewahren Sie das Gerät bei Nichtverwendung in einer geeigneten antistatischen Verpackung auf.

ACHTUNG

Schmutzschutzstreifen

Entfernen Sie den Schmutzschutzstreifen erst, wenn die Steuerung und alle anderen Komponenten in der Nähe der Steuerung montiert sind und die Verdrahtung abgeschlossen ist.

Nach Abschluss der Verdrahtung können Sie den Schmutzschutzstreifen entfernen. Wenn Sie den Streifen nicht vor der Inbetriebnahme entfernen, kann es zu einer Überhitzung kommen.

ACHTUNG

Der Ausfall erforderlicher Sicherheitsfunktionen kann zu schweren Verletzungen führen.

- Verwenden Sie Testausgänge nicht als Sicherheitsausgänge.
- Verwenden Sie weder DeviceNet-Standard-E/A-Daten noch explizite Nachrichtendaten als Sicherheitsdaten.
- Verwenden Sie Statusanzeigen nicht für Sicherheitsvorgänge.
- Schließen Sie an den Sicherheits- oder Testausgängen keine Lasten an, die über dem Bemessungswert liegen.
- Verdrahten Sie die Steuerung ordnungsgemäß, sodass die 24V DC-Leitung nicht versehentlich die Ausgänge berührt.
- Erden Sie die 0-V-Leitung der Stromversorgung für externe Ausgangsgeräte, sodass diese Geräte nicht eingeschaltet werden, wenn die Leitung des Sicherheits- oder Testausgangs geerdet wird.
- Die Steuerung darf weder geöffnet noch repariert oder verändert werden. Andernfalls könnten die Sicherheitsfunktionen beeinträchtigt werden.

Die Netzknotenadressierung

Jedes Gerät benötigt für die Kommunikation im DeviceNet-Netzwerk eine eigene Adresse. Wenden Sie die unten stehenden Empfehlungen beim Zuordnen von Adressen zu den Geräten im Netzwerk an.

Empfehlungen für Netzknotenadressen

Gerät	Adresse	Hinweise
Scanner	0	Wenn Sie über mehrere Scanner verfügen, weisen Sie diesen nacheinander die niedrigsten Adressen zu.
Alle Geräte im Netzwerk mit Ausnahme des Scanners	1 bis 61	Lücken zwischen den Adressen sind zulässig und haben keine Auswirkungen auf die Systemleistung. Wenn Sie Adressen frei lassen, sind Sie bei einer späteren Erweiterung des Systems flexibler.
RSNetWorx for DeviceNet-Workstation	62	Wenn Sie einen Computer direkt mit dem DeviceNet-Netzwerk verbinden, verwenden Sie für diesen Computer oder das Bridging- bzw. Verbindungsgerät die Adresse 62.
Kein Gerät	63	Lassen Sie die Adresse 63 frei. Dies ist die Adresse, an der ein nicht in Betrieb befindlicher Knoten im Allgemeinen in das Netzwerk eingefügt wird.

Das DeviceNet-Standardnetzwerk weist die Prioritäten bei der Kommunikation anhand der Netzknotennummer des Geräts zu. Je niedriger die Nummer, desto höher ist die Kommunikationspriorität des Geräts. Diese Priorität ist wichtig, wenn mehrere Knoten versuchen, gleichzeitig im Netzwerk zu kommunizieren.

DeviceNet-Sicherheitsknoten verfügen im Netzwerk unabhängig von ihrer Netzknotennummer über eine höhere Priorität. Die DeviceNet-Sicherheitskommunikation von Geräten mit niedrigeren Netzknotennummern hat eine höhere Priorität als die von Geräten mit einer höheren Netzknotennummer.

Festlegen der Netzknotenadresse

Legen Sie die Netzwerknotenadresse fest, bevor Sie die Steuerung montieren.

WICHTIG

Schalten Sie die Steuerung aus, bevor Sie die Netzwerknotenadresse oder die Kommunikationsgeschwindigkeit über die Schalter festlegen.

Ändern Sie die Schalterstellungen nicht bei eingeschalteter Stromversorgung. Die Steuerung erkennt die Änderung an der Konfiguration automatisch und wechselt in den Modus ABORT (Abbrechen).

Verwenden Sie für das Einstellen der Netzknotenadressen mithilfe der zwei Drehschalter an der Frontabdeckung der Steuerung einen kleinen Schlitzschraubendreher. Gehen Sie vorsichtig vor, um die Schalter nicht zu zerkratzen. Es sind die Werte zwischen 00 und 63 zulässig. Die Standardeinstellung ist 63.

Gehen Sie zum Festlegen der Netzknotenadresse folgendermaßen vor.

1. Legen Sie die Zehnerstelle der Netzknotenadresse (dezimal) durch Drehen des linken Drehschalters fest.

2. Legen Sie die Einerstelle durch Drehen des rechten Drehschalters fest.

3. Wenn die Netzknotenadresse mit RSNetworx for DeviceNet festgelegt werden soll, stellen Sie die Drehschalter auf einen Wert zwischen 64 und 99 ein.

WICHTIG Es tritt ein Fehler auf, wenn eine Netzknotenadresse mehrmals festgelegt wird.

Festlegen der Kommunikationsgeschwindigkeit

Legen Sie die Kommunikationsgeschwindigkeit fest, bevor Sie die Steuerung montieren.

WICHTIG Schalten Sie die Steuerung aus, bevor Sie die Netzwerknotenadresse oder die Kommunikationsgeschwindigkeit über die Schalter festlegen.

Ändern Sie die Schalterstellungen nicht bei eingeschalteter Stromversorgung. Die Steuerung erkennt die Änderung an der Konfiguration automatisch und wechselt in den Modus ABORT (Abbrechen).

DeviceNet-Kommunikation

Die Standardkommunikationsgeschwindigkeit für ein DeviceNet-Netzwerk beträgt 125 kbit/s.

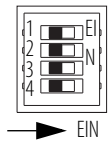
Wenn Sie eine andere Kommunikationsgeschwindigkeit verwenden möchten, bestimmen Hauptleitungslänge und Kabeltypen welche Kommunikationsgeschwindigkeiten die Anwendung unterstützt.

DeviceNet-Kommunikationsgeschwindigkeiten und -Kabellängen

Kommunikations-geschwindigkeit	Maximale Länge			Kumulative Länge der Stichleitung
	Flachkabel	Dickes Kabel	Dünnes Kabel	
125 kbit/s	420 m	500 m	100 m	156 m
250 kbit/s	200 m	250 m	100 m	78 m
500 kbit/s	75 m	100 m	100 m	39 m

Legen Sie die Kommunikationsgeschwindigkeit mit dem DIP-Schalter an der Vorderseite der Steuerung fest.

DIP-Schalter für die Kommunikationsgeschwindigkeit



Einstellungen der DIP-Schalter

DIP-Schalterstift				Kommunikationsgeschwindigkeit
1	2	3	4	
AUS	AUS	AUS	AUS	125 kbit/s
EIN	AUS	AUS	AUS	250 kbit/s
AUS	EIN	AUS	AUS	500 kbit/s
EIN	EIN	AUS	AUS	Festgelegt durch Software
EIN oder AUS	EIN oder AUS	EIN	AUS	Festgelegt durch Software
EIN oder AUS	EIN oder AUS	EIN oder AUS	EIN	Automatische Baudratenerkennung

WICHTIG Wenn Sie die Kommunikationsgeschwindigkeit im Netzwerk ändern, müssen Sie sicherstellen, dass alle Geräte entsprechend der neuen Kommunikationsgeschwindigkeit geändert werden. Unterschiedliche Kommunikationsgeschwindigkeiten führen zu Kommunikationsfehlern.

Wenn Sie für andere Geräte die automatische Baudratenerkennung einstellen, muss für mindestens ein Gerät im Netzwerk eine Kommunikationsgeschwindigkeit festgelegt worden sein. Wenn Sie für alle Geräte die automatische Baudratenerkennung einstellen, können diese keine Kommunikationsgeschwindigkeit festlegen und daher nicht miteinander kommunizieren.

Ethernet-Kommunikation

Es wird empfohlen, das Modul über einen 100-Mbit/s-Ethernet-Switch am Netzwerk anzuschließen, wodurch Kollisionen und verlorene Datenpakete verringert sowie die Bandbreite erhöht werden kann.

Im Auslieferungszustand ist BOOTP in der Steuerung 1752-L24BBBE zum Festlegen der IP-Adresse aktiviert. Sie können jeden beliebigen im Handel erhältlichen BOOTP-Server verwenden. Wenn Ihr Netzwerk nicht über BOOTP-Server-Fähigkeiten verfügt, laden Sie den kostenlosen BOOTP-Server von Rockwell Automation von folgender Adresse herunter: http://www.rockwellautomation.com/rockwellsoftware/download/.

Informationen zum Festlegen der IP-Adresse mithilfe des BOOTP-Dienstprogramms von Rockwell Automation finden Sie auf Seite 54.

Die folgende Tabelle enthält zusätzliche Informationen zu EtherNet/IP.

Ausführliche Informationen zur EtherNet/IP-Kommunikation finden Sie in der Publikation ENET-AP001, EtherNet/IP Performance and Application Solution.

EtherNet/IP – Allgemeine Informationen

Attribut	Wert
Anzahl der CIP-Pakete	2
Übertragungsleistung der Einheit	3000 pps(1)
Kommunikation expliziter Nachrichten	502 B(2)

(1) PPS = Pakete pro Sekunde. Gibt die Anzahl der Sende- oder Empfangspakete an, die pro Sekunde verarbeitet werden können.

(2) Die maximale Nachrichtenlänge für eine Verbindung der Klasse 3 und eine UCMM-Verbindung.

Montage der SmartGuard-Steuerung

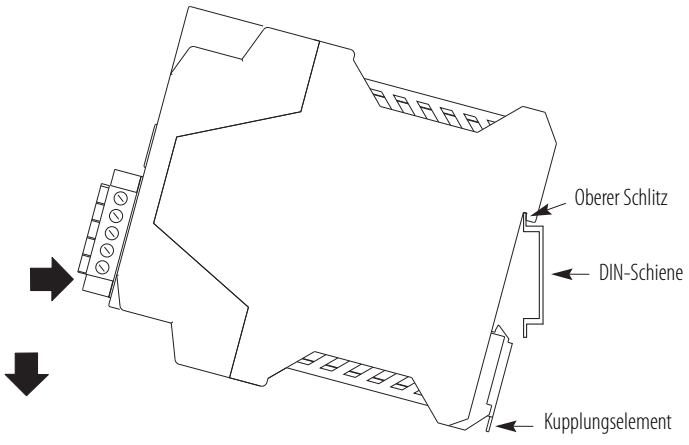
WICHTIG

Beachten Sie für eine effektive Kühlung Folgendes:

- Montieren Sie die Steuerung an einer horizontalen DIN-Schiene. Montieren Sie die Steuerung nicht vertikal.
- Lassen Sie mindestens 50 mm über und unter der Steuerung und 5 mm an beiden Seiten Platz.
- Wählen Sie einen Standort mit Luftzirkulation, oder verwenden Sie zusätzlich einen Lüfter.
- Montieren Sie die Steuerung nicht über einer Heizung.

Die Steuerung kann nicht in einem Schaltschrank montiert werden.
Gehen Sie zum Montieren der Steuerung an einer EN50022-35x7,5- oder einer EN50022-35x15-DIN-Schiene folgendermaßen vor.

1. Haken Sie den oberen Schlitz auf der DIN-Schiene ein.
2. Lassen Sie den unteren Teil der Steuerung einrasten, während Sie die Steuerung gegen den oberen Teil der Schiene drücken.



3. Bringen Sie die Endplatten an beiden Enden der DIN-Schiene an.

Nehmen Sie die Steuerung von der DIN-Schiene ab. Ziehen Sie hierfür mit einem Schlitzschraubendreher das Kupplungselement nach unten, und heben Sie die Steuerung von der Schiene. Die Steuerung 1752-L24BBB verfügt über ein Kupplungselement und die Steuerung 1752-L24BBBE über zwei Kupplungselemente am Boden der Steuerung.

Erden der SmartGuard-Steuerung

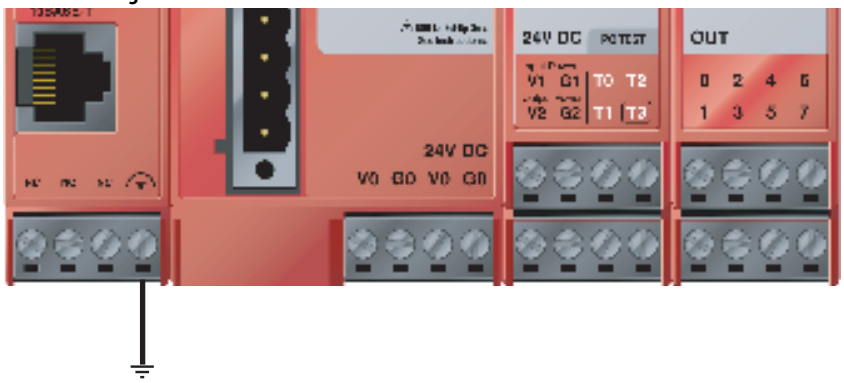
ACHTUNG

Dieses Produkt ist über die DIN-Schiene an der Chassiserdung geerdet. Verwenden Sie eine verzinkte, gelb chromatierte DIN-Schiene aus Stahl, um eine ordnungsgemäße Erdung zu gewährleisten. Die Verwendung anderer DIN-Schienenmaterialien (z. B. Aluminium oder Kunststoff), die korrodieren oder oxidieren können oder schlechte Leiter sind, kann zu einer mangelhaften oder unstetigen Erdung führen. Sichern Sie die DIN-Schiene an der Montagefläche etwa alle 200 mm und verwenden Sie entsprechende Arretierstücke.

Sie müssen alle Geräte der Anwendung ausreichend erden. Es bietet sich an, die Steuerung über den V0/G0-Stromanschluss zu erden.

Wenn Sie die Steuerung 1752-L24BBBE verwenden, müssen Sie außerdem die Ethernet-Erdungsklemme an einer zulässigen Erdung anschließen.

Ethernet-Erdung



Weitere Informationen finden Sie in den Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1.

Anschließen der Stromversorgung

Die Steuerung wird über eine externe 24-V-DC-Spannungsquelle mit Strom versorgt. Die Ausgangs-Haltezeit muss mindestens 20 ms betragen.

Zur Einhaltung der CE-Niederspannungsrichtlinie müssen DeviceNet-Verbindungen und -Eingänge/Ausgänge durch eine DC-Spannungsquelle mit Sicherheits-Kleinspannung (SELV) oder Schutz-Kleinspannung (PELV) mit Strom versorgt werden.

Zur Einhaltung der UL-Einschränkungen müssen DeviceNet-Verbindungen und -Eingänge/Ausgänge durch eine DC-Spannungsquelle mit Strom versorgt werden, deren Sekundärstromkreise vom Primärstromkreis durch doppelte Isolierung oder verstärkte Isolierung getrennt sind. Die DC-Spannungsquelle muss den Anforderungen für Stromkreise der Klasse 2 oder Stromkreisen mit begrenzter Spannung/Stromstärke gemäß UL 508 entsprechen.

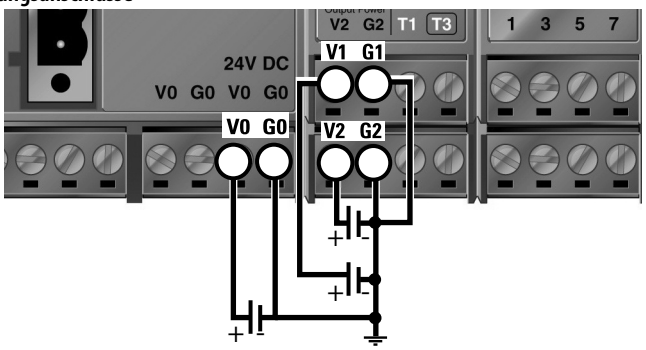
TIPP

Die folgenden 1606-Netzteile von Rockwell Automation sind SELV- und PELV-konform und entsprechen den Anforderungen an Isolierung und Ausgangs-Haltezeit der SmartGuard 600-Steuerung:

- 1606-XLP30E
- 1606-XLP50E
- 1606-XLP50EZ
- 1606-XLP72E
- 1606-XLP95E
- 1606-XLDNET4
- 1606-XLSDNET4

Die SmartGuard-Steuerung verfügt über drei V/G-Klemmenpaare, die eine Stromversorgung erfordern. Es sind zwar zwei V0/G0-Paare vorhanden, aber da diese intern miteinander verbunden sind, müssen Sie nur ein V0/G0-Paar anschließen. Das andere Paar können Sie zur Stromverteilung an andere Geräte verwenden.

Stromversorgungsanschlüsse



Herstellen von Kommunikationsverbindungen

WARNUNG

Sie sollten das Kommunikationskabel weder einstecken noch herausziehen, während die Steuerung oder ein anderes Gerät im Netzwerk eingeschaltet ist, weil dabei ein elektrischer Lichtbogen entstehen kann. Dies kann bei Installationen an explosionsgefährdeten Standorten eine Explosion verursachen. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

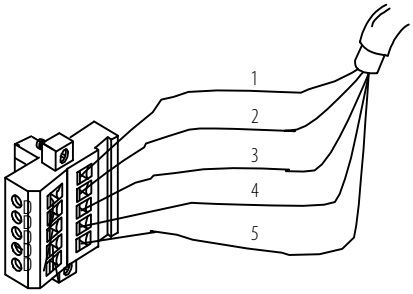
Sie können das Netzwerk und die Steuerung im DeviceNet-Netzwerk über eine 1784-PCD-Karte im PC mit der Software RSNetWorx for DeviceNet konfigurieren. Die Konfiguration von Netzwerk und Steuerung mit der Software RSNetWorx for DeviceNet ist auch über den USB-Anschluss möglich. Außerdem können Sie die Steuerung mithilfe der Software RSNetWorx for DeviceNet konfigurieren, indem Sie eine Verbindung mit dem EtherNet/IP-Port herstellen und ein Routing bis zum DeviceNet-Netzwerk vornehmen.

Anschließen an den DeviceNet-Anschluss

Gehen Sie beim Anschließen an den DeviceNet-Anschluss folgendermaßen vor.

1. Nehmen Sie die Verdrahtung entsprechend den Farben auf dem Anschluss vor.

Draht-belegung	Drahtfarbe	Anschluss an
V+	Rot	V+
CAN H	Weiß	CAN H
Beilaufdraht	–	Beilaufdraht
CAN L	Blau	CAN L
V–	Schwarz	V–



2. Schließen Sie den Verbinder an den DeviceNet-Anschluss an.

3. Ziehen Sie die Schrauben mit einem Drehmoment von 0,25 bis 0,3 Nm fest.

Einzelheiten zum DeviceNet-Anschluss finden Sie in Publikation DNET-UM072, DeviceNet Media Design Installation Guide. Lesen Sie außerdem die Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1.

Verbinden mit dem USB-Anschluss

Verbinden Sie den USB-Kommunikationsanschluss mit dem PC, wenn Sie das Netzwerk und die Steuerung mit RSNetWorx for DeviceNet konfigurieren möchten. Verwenden Sie für die Verbindung ein handelsübliches USB-A-zu-USB-B-Kabel (Stecker/Stecker).

ACHTUNG

Um elektromagnetische Störungen zu vermeiden, sollte das USB-Kabel nicht länger als 3 m sein.

Der USB-Anschluss ist für zeitweilige Programmierzwecke vorgesehen, nicht für eine dauerhafte Verbindung.

WARNUNG

Wenn Sie das USB-Kabel einstecken oder abziehen, während das Modul oder ein anderes Gerät im USB-Netzwerk eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. Dies kann bei Installationen an explosionsgefährdeten Standorten eine Explosion verursachen. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

Verbinden mit dem DeviceNet-Anschluss

Abhängig davon, wo Sie Ihr Kabel verlegen möchten, müssen Sie ein für die Umgebung geeignetes Kabel auswählen. Abgeschirmte Kabel bieten in Industrieumgebungen eine bessere Leistung als nicht abgeschirmte Kabel. Wenn Ihre Anwendung in einer stark störungsbehafteten Umgebung eingesetzt wird oder Ihr Kabel in der Nähe von Quellen mit Störstrahlung verlegt werden soll, müssen Sie die Verwendung abgeschirmter Kabel in Betracht ziehen.

Verwenden Sie abgeschirmte Kabel, wenn Ihre Anwendung mindestens eines der folgenden Elemente aufweist:

- Punktschweißsteuerung
- Motor Control Center (MCC)
- Antriebe mit mehr als 10 HP
- Induktionsschweißverfahren
- Nähe zu starker Hochfrequenzstrahlung
- Elektrostatische Verfahren
- Starkstromgeräte (mit mehr als 100 A)

WICHTIG

Abschirmungen spielen eine wichtige Rolle, wenn Ihre Systeme Störfestigkeit aufweisen müssen. Allerdings kann ein falsch installiertes abgeschirmtes Kabel aufgrund von Spannungsverschiebungen in Ihrem Erdungssystem auch zu Problemen führen. Um die Auswirkungen des Masseversatzes zu minimieren, müssen Sie die Abschirmung an einem Ende des Kabels isolieren. In diesem Fall muss die Abschirmung am Gerät und nicht am Switch isoliert werden.

Verwenden Sie zum Anschließen der Steuerung an das EtherNet/IP-Netzwerk einen RJ45-Stecker. Wenn Sie die SmartGuard-Steuerung an einen Switch oder Hub anschließen, verwenden Sie ein Standard-Ethernet-Kabel. Wenn Sie die SmartGuard-Steuerung direkt an Ihren PC oder an eine NIC-Karte anschließen, verwenden Sie ein Übergangskabel (Nullmodemkabel).

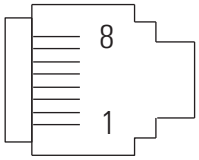
ACHTUNG

Das Kabel zwischen Hub und Knoten darf maximal 100 m lang sein.

WARNUNG

Wenn Sie das Ethernet-Kabel anschließen oder abziehen, solange diese Steuerung oder ein anderes Gerät in diesem Netzwerk eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. Dies kann bei Installationen an explosionsgefährdeten Standorten eine Explosion verursachen. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

Positionen der Ethernet-Stifte

Stift Nr.	Name des Stifts	Position des Stifts
8	Nicht verwendet	
7	Nicht verwendet	
6	RD–	
5	Nicht verwendet	
4	Nicht verwendet	
3	RD+	
2	TD–	
1	TD+	

Verdrahten der SmartGuard 600-Steuerung

Verwenden Sie Kabel mit einer Länge von maximal 30 m.

Allgemeine Informationen zur Verdrahtung

Attribute	Wert
Drahttyp	Kupfer
Verdrahtungskategorie(1)	2 – an Strom-, Signal- und Kommunikationsanschlüssen
Leiterquerschnitt	Verwenden Sie für die Stromversorgung und Ein- und Ausgänge massive Drähte mit 0,2 bis 2,5 mm^2 (AWG 12 bis 24) oder verseilte, flexible Drähte mit 0,34 bis 1,5 mm^2 (AWG 16 bis 22). Bereiten Sie verseilte Kabel vor dem Verdrahten vor, indem Sie diese mit Terminierungshülsen mit Kunststoffisolierung (gemäß Standard DIN 46228-4) versehen.
Anzugsmoment der E/A-Klemmenschrauben	0,56 bis 0,79 Nm

(1) Planen Sie mithilfe dieser Informationen zur Leitungskategorie die Verlegung der Leiter. Siehe die Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1.

Beschreibung der Klemmen der Steuerung

Klemmenbezeichnung	Beschreibung
V0	Netzklemme für den internen Schaltkreis (Logik).
G0	Netzklemme für den internen Schaltkreis (Logik).
V1	Netzklemme für Eingangsschaltkreise und Testausgänge.
G1	Netzklemme für Eingangsschaltkreise und Testausgänge.
V2	Netzklemme für Sicherheitsausgänge.
G2	Netzklemme für Sicherheitsausgänge.
IN0–IN15	Klemmen für Sicherheitseingänge.
T0–T3	Testausgangsklemmen, über die Impulstestquellen für die Sicherheitseingänge IN0 bis IN15 bereitgestellt werden können. T3 kann auch zur Erkennung nicht angeschlossener Kabel und durchgebrannter Lampen, beispielsweise für eine Muting-Lampe, verwendet werden.
OUT0–OUT7	Klemmen für Sicherheitsausgänge.

WARNUNG

Wenn Sie einen Draht anschließen oder entfernen, während die Stromversorgung eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. Dies kann bei Installationen an explosionsgefährdeten Standorten eine Explosion verursachen. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

WARNUNG

Wenn Sie die abnehmbaren Klemmenleiste (RTB) anschließen oder entfernen, während die feldseitige Stromversorgung eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. Dies kann bei Installationen an explosionsgefährdeten Standorten eine Explosion verursachen. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

WICHTIG

Bereiten Sie verseilte Kabel vor, indem Sie diese mit Terminierungshülsen mit Kunststoffisolierung (gemäß Standard DIN 46228-4) versehen. Ähnliche Hülsen, die jedoch nicht diesen Standard erfüllen, passen evtl. nicht an die Klemmenleiste der Steuerung.

Verdrahten von Eingangsgeräten

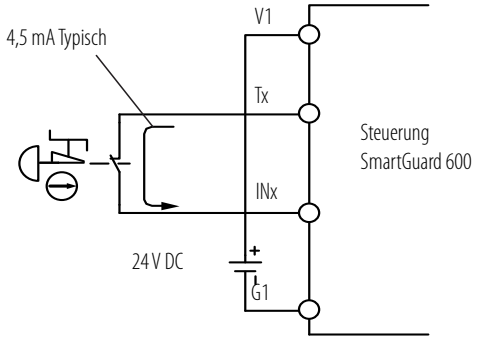
ACHTUNG

Das Anlegen einer ungeeigneten DC- oder AC-Spannung kann zu einem Verlust der Sicherheitsfunktion, zur Beschädigung des Produkts und zu schweren Verletzungen führen. Verwenden Sie ausschließlich geeignete Spannungen auf den Steuerungseingängen.

Eingangsgeräte mit mechanischen Kontaktausgängen, z. B. Not-Aus-Schalter oder Sicherheits-Endschalter, verwenden sowohl eine Sicherheitseingangsklemme als auch eine Testausgangsklemme. Damit erfüllt der Schaltkreis die Anforderungen der Kategorie 4.

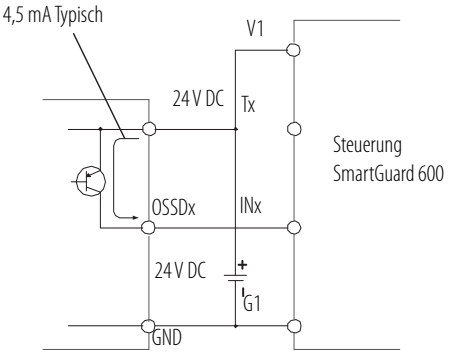
Wenn Sicherheitskomponenten und -systeme über Testausgänge mit einer Eingangsschaltung an die SmartGuard-Steuerung angeschlossen werden sollen, wird eine Kabellänge von maximal 30 m empfohlen.

Eingangsgeräte mit mechanischen Kontaktausgängen



Geräte, wie z. B. Lichtgitter, mit stromliefernden PNP-Halbleiterausgängen senden ein Signal an den Sicherheitseingang der SmartGuard 600-Steuerung und verwenden keinen Testausgang.

Eingangsgeräte mit PNP-Halbleiterausgängen



Verdrahten von Ausgangsgeräten

ACHTUNG

Schwere Verletzungen können die Folge sein, wenn die vorgeschriebenen Sicherheitsfunktionen nicht einwandfrei arbeiten.

Schließen Sie an Sicherheits- und Testausgängen niemals Lasten an, die über dem Nennwert des betreffenden Ausgangs liegen.

Verwenden Sie Testausgänge nicht als Sicherheitsausgänge.

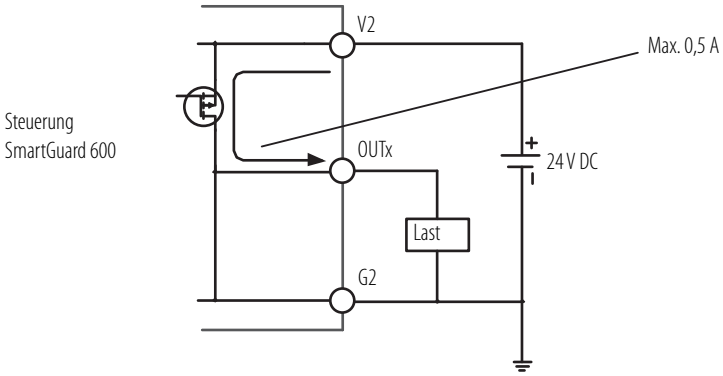
Verdrahten Sie die Steuerung ordnungsgemäß, und achten Sie darauf, dass die 24-V-DC-Leitungen keinen Kontakt mit den Sicherheits- oder Testausgängen haben.

Verbinden Sie die Stromversorgung nicht mit den Testausgangsklemmen.

Erden Sie die 0-V-Leitung der Stromversorgung für externe Ausgangsgeräte, sodass diese Geräte nicht durch das Erden der Sicherheits- oder Testausgangsleitung eingeschaltet werden.

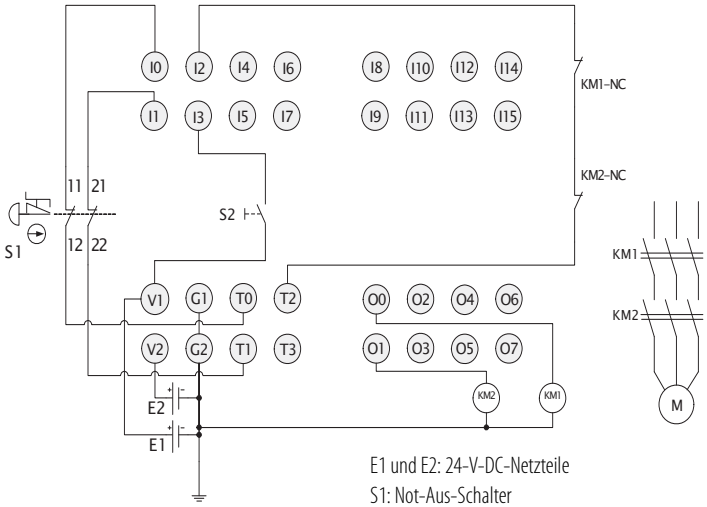
Trennen Sie E/A-Kabel von Hochspannungs- und Hochstromleitungen.

Verdrahtung von Ausgangsgeräten



Verdrahtungsbeispiele

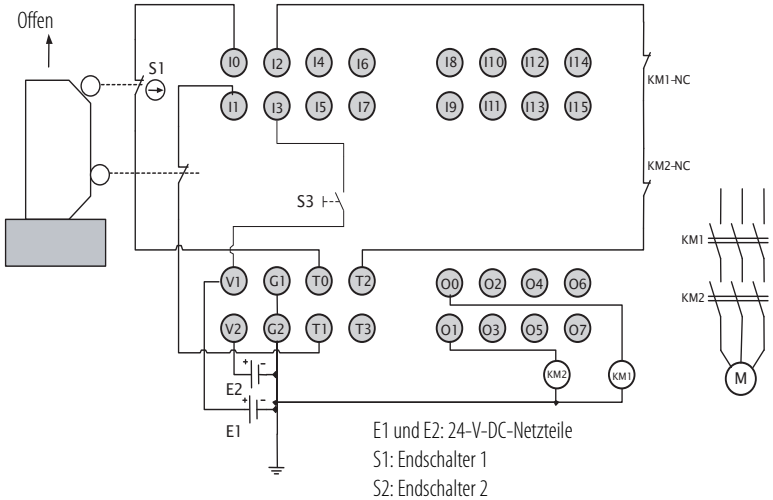
Not-Aus-Schalter



E1 und E2: 24-V-DC-Netzteile
S1: Not-Aus-Schalter
S2: Rücksetzschalter (Schließer-Kontakt)
KM1 und KM2: Schütze

Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

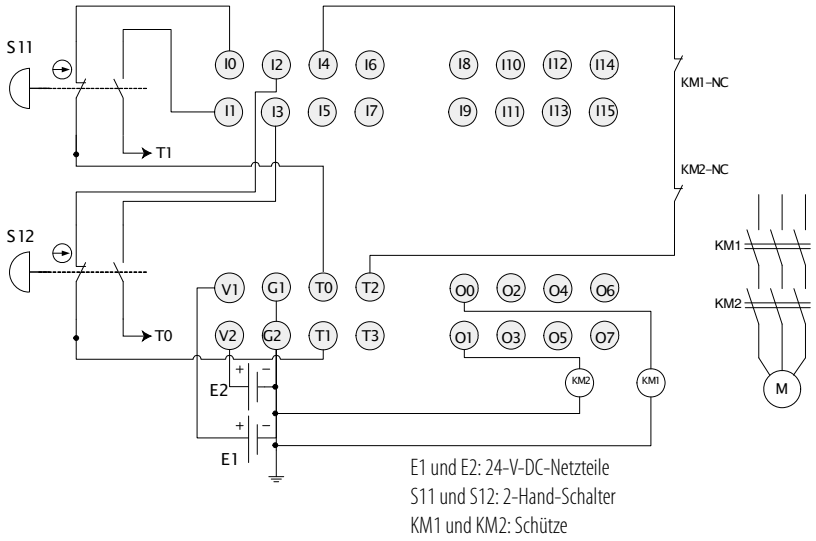
Sicherheitstür



E1 und E2: 24-V-DC-Netzteile
S1: Endschalter 1
S2: Endschalter 2
S3: Rücksetzschalter
KM1 und KM2: Schütze

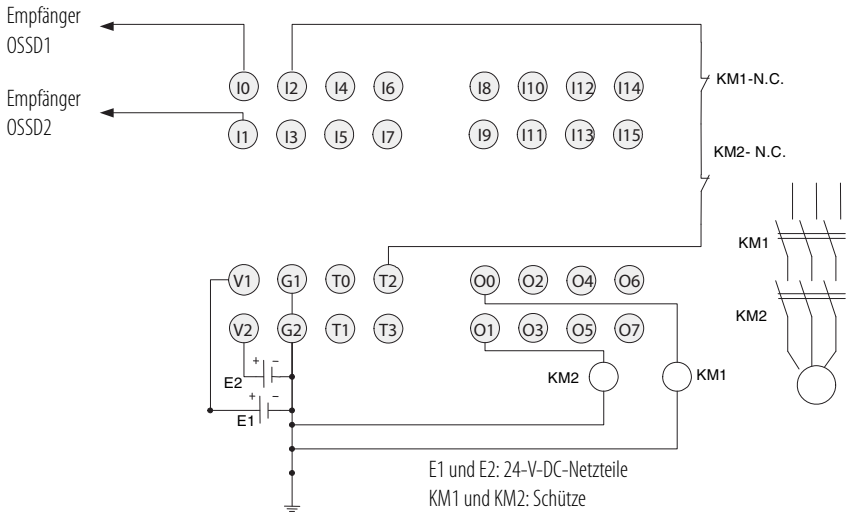
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

2-Hand-Schalter



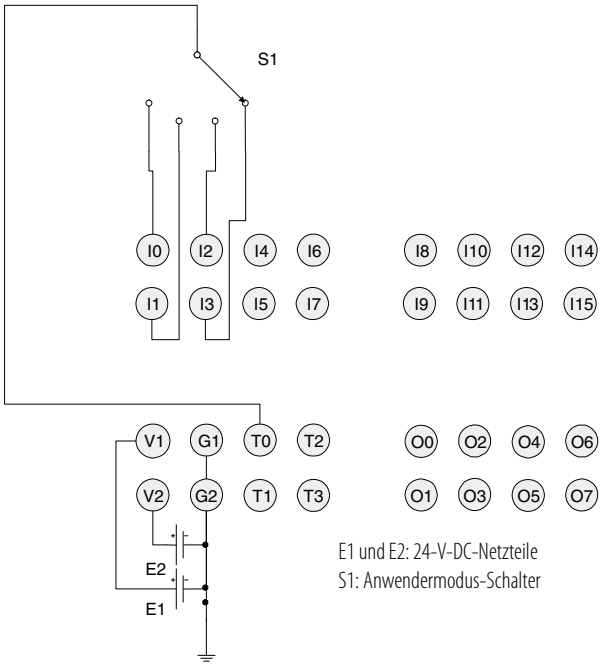
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Lichtgitter



Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Anwendermodus-Schalter



E1 und E2: 24-V-DC-Netzteile
S1: Anwendermodus-Schalter

Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Einrichten Ihres DeviceNet-Netzwerks

Einleitung

Thema	Seite
Anschließen eines Computers an das DeviceNet-Netzwerk	41
Inbetriebnahme aller Netzknoten	42
Durchsuchen des Netzwerks	44
Konfigurationssignatur	45
Sicherheits-Reset (optional)	46
Festlegen von Kennwörtern (optional)	47

Anschließen eines Computers an das DeviceNet-Netzwerk

Führen Sie einen der beiden folgenden Schritte durch, um auf ein Netzwerk zuzugreifen:

- Stellen Sie eine direkte Verbindung zum Netzwerk her.
- Stellen Sie eine Verbindung zu einem anderen Netzwerk her, und suchen Sie über einen Koppler nach dem gewünschten Netzwerk.

TIPP

Sie können mithilfe des USB-Anschlusses der SmartGuard-Steuerung nach dem DeviceNet- oder EtherNet/IP-Netzwerk suchen.

Die Bridging-Funktion von SmartGuard-USB zu DeviceNet ist eingeschränkt. So können beispielsweise weder ein 1734-ADN-Modul noch POINT I/O-Module konfiguriert werden. Zudem können 1753-DNSI-Module nicht über die SmartGuard-Steuerung konfiguriert werden. Verwenden Sie für diese Vorgänge stattdessen eine 1784-PCD-Karte.

Führen Sie im Anschluss an die Auswahl eines Netzwerks folgende Schritte durch:

- Sofern erforderlich, Installation der Kommunikationskarte.
- Ermitteln von Netzwerkparametern für den Computer, z. B. eine Netzwerkadresse.
- Anschließen des Computers am Netzwerk mithilfe des Verbindungskabels.

WICHTIG

Beim erstmaligen Anschluss einer SmartGuard-Steuerung an Ihren Computer über den USB-Anschluss wird unter Windows die Geräteerkennung durchlaufen. Sie werden aufgefordert, USB-Treiber anzugeben. Der Treiber befindet sich auf der RSLinx Classic-CD im Ordner „SmartGuardUSB-KernelDrivers“.

Konfigurieren des Treibers für das Netzwerk

1. Starten Sie die Software RSLinx.
2. Klicken Sie auf „Configure Driver“ (Treiber konfigurieren).
3. Fügen Sie aus der Pulldown-Liste der verfügbaren Treibertypen (Available Driver Types) den Treiber für Ihr Netzwerk hinzu.

Netzwerk	Treiber
RS-232	RS-232-DF1-Geräte
EtherNet/IP	Ethernet-Geräte
DeviceNet	DeviceNet-Treiber
USB	SmartGuard-USB-Treiber

4. Konfigurieren Sie den Treiber.

   Die vorzunehmenden Einstellungen sind abhängig vom ausgewählten Netzwerk und der Entscheidung, ob eine Kommunikationskarte oder ein Schnittstellenmodul verwendet werden soll.

Stellen Sie sicher, dass der Treiber funktioniert

1. Überprüfen Sie das Dialogfeld „Configure Drivers“ (Treiber konfigurieren), um sicherzustellen, dass der Treiber ausgeführt wird.
2. Schließen Sie das Dialogfeld.
3. Öffnen Sie das Dialogfeld „RSWho“.
4. Doppelklicken Sie auf den Treiber, um das Netzwerk anzuzeigen.

Inbetriebnahme aller Netzknoten

Wenn Sie die Netzknotenadresse und Kommunikationsgeschwindigkeit Ihrer Geräte nicht mithilfe von Hardware-Schaltern eingerichtet haben, müssen die einzelnen Geräte mithilfe der Software RSNetWorx for DeviceNet in Betrieb genommen werden.

Bevor Sie das Werkzeug zur Inbetriebnahme der Netzknoten (Node Commissioning Tool) von RSNetWorx for DeviceNet verwenden können, müssen Ihr Computer und die DeviceNet-Geräte mit dem DeviceNet-Netzwerk verbunden worden sein.

Verwenden Sie das Node Commissioning Tool von RSNetWorx for DeviceNet, um die Netzknotenadresse und/oder die Kommunikationsgeschwindigkeit der SmartGuard-Steuerung und anderer DeviceNet-Geräte festzulegen.

Befolgen Sie bei der Auswahl der Netzknotenadressen für Ihr DeviceNet-Netzwerk die Richtlinien auf Seite 26.

WICHTIG

Damit die Netznotenadresse mithilfe des Node Commissioning Tool der Software RSNetWorx for DeviceNet festgelegt werden kann, muss der Drehschalter für die Netzknotenadresse an der Steuerung auf einen Wert zwischen 64 und 99 eingestellt werden.

Weitere Informationen zum Einstellen der Netzknotenadresse mithilfe des Drehschalters finden Sie auf Seite 26.

Führen Sie folgende Schritte durch, um das Node Commissioning Tool zu verwenden.

1. Wählen Sie in RSNetWorx for DeviceNet „Tools > Node Commissioning“ (Werkzeuge > Inbetriebnahme der Netzknoten) aus.
2. Klicken Sie im Dialogfeld „Node Commissioning“ (Inbetriebnahme der Netzknoten) auf „Browse“ (Durchsuchen), um im Netzwerk nach einem Gerät zu suchen.

   Sie können den SmartGuard-USB-Anschluss oder den Ethernet/IP-Anschluss durchsuchen, um zum DeviceNet-Anschluss zu gelangen.
3. Wählen Sie im linken Bereich das DeviceNet-Netzwerk aus.
4. Klicken Sie im rechten Bereich das in Betrieb zu nehmende Gerät aus, und klicken Sie auf „OK“.
5. Wenn die Kommunikationsgeschwindigkeit geändert werden soll, wählen Sie den gewünschten Wert aus.

   WICHTIG

   Die Kommunikationsgeschwindigkeit des Geräts wird erst aktualisiert, wenn dieses aus- und eingeschaltet oder zurückgesetzt wird.
6. Geben Sie im Dialogfeld „Node Commissioning“ (Inbetriebnahme der Netzknoten) die neue Adresse des Geräts ein und klicken Sie auf „Apply“ (Übernehmen).

   Eine Bestätigungsmeldung informiert Sie darüber, ob der Vorgang erfolgreich war.

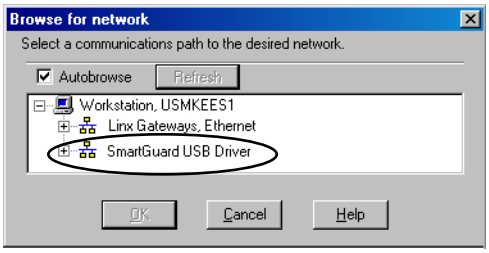
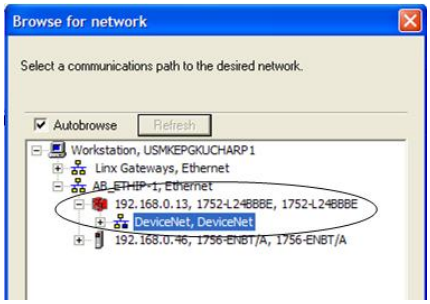
   WICHTIG

   Um die Netzknotenadresse eines Sicherheitsgeräts zu ändern, müssen Sie zunächst die Sicherheitsnetzwerknummer (SNN) mithilfe einer Sicherheitsrücksetzung auf einen nicht initialisierten Status zurücksetzen (siehe Beschreibung auf Seite 46).

Durchsuchen des Netzwerks

Führen Sie folgende Schritte durch, um das Netzwerk zu durchsuchen.

1. Ermitteln Sie Ihren Verbindungstyp.

Verwendeter Verbindungstyp	Vorgehensweise
DeviceNet-Netzwerk	Wechseln Sie zu Schritt 2.
USB-Anschluss	Führen Sie folgende Schritte durch, um einen Pfad zum DeviceNet-Netzwerk zu konfigurieren. A. Wählen Sie im Menü „Network" (Netzwerk) die Option „Properties" (Eigenschaften) aus. B. Klicken Sie im Dialogfeld „DeviceNet" auf „Set Online Path" (Online-Pfad festlegen). C. Wählen Sie im Dialogfeld „Browse for Network" (Nach Netzwerk suchen) den gewünschten Pfad aus und klicken Sie auf „OK". 
EtherNet/IP-Netzwerk	Führen Sie folgende Schritte durch, um einen Pfad zum DeviceNet-Netzwerk zu konfigurieren. A. Wählen Sie im Menü „Network" (Netzwerk) die Option „Properties" (Eigenschaften) aus. B. Klicken Sie im Dialogfeld „DeviceNet" auf „Set Online Path" (Online-Pfad festlegen). C. Wählen Sie im Dialogfeld „Browse for Network" (Nach Netzwerk suchen) den gewünschten Pfad aus und klicken Sie auf „OK". 

2. Klicken Sie auf das Online-Symbol .

3. Warten Sie, bis die Netzwerksuche abgeschlossen wurde.

   Beim Durchsuchen des Netzwerks werden alle Geräte im Netzwerk in RSNetWorx for DeviceNet angezeigt.

4. Überprüfen Sie, ob all Ihre Netzknoten angezeigt werden.

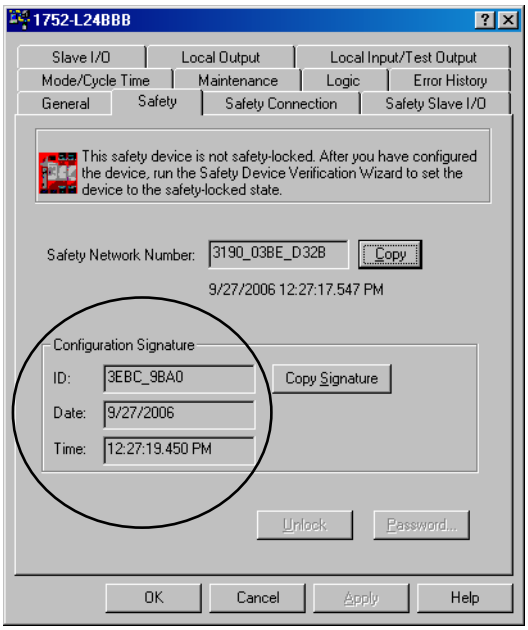
5. Speichern Sie Ihr Projekt in RSNetWorx for DeviceNet.

Konfigurationssignatur

Jedes Sicherheitsgerät verfügt über eine eindeutige Konfigurationssignatur, mit der die Konfiguration identifiziert wird, um die Integrität der Konfigurationsdaten bei Downloads, beim Verbindungsaufbau und beim Ersetzen von Modulen zu überprüfen.

Die Konfigurationssignatur besteht aus einer ID-Nummer, einem Datum und einer Uhrzeit. Sie wird in RSNetWorx for DeviceNet automatisch erstellt, wenn auf das Gerät eine Konfigurationsaktualisierung angewendet wird. Die Konfigurationssignatur finden Sie im Dialogfeld „Device Properties“ (Geräteeigenschaften) auf der Registerkarte „Safety“ (Sicherheit). Sie wird außerdem Zeichen für Zeichen auf der alphanumerischen Anzeige angezeigt, wenn der Service-Schalter gedrückt wird.

Konfigurationssignatur der Steuerung SmartGuard 600

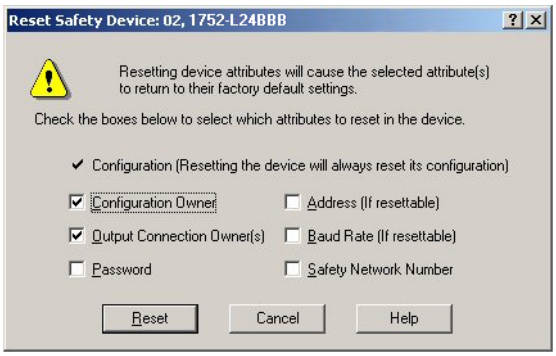


Die Konfigurationssignatur wird bei jedem Suchvorgang und jeweils beim Öffnen des Dialogfelds „Device Properties“ (Geräteeigenschaften) gelesen, sofern sich die Software im Online-Modus befindet. In RSNetWorx for DeviceNet wird die Konfigurationssignatur der Gerätekonfigurationsdatei der Software (offline) mit der Konfigurationssignatur des Online-Geräts verglichen. Wenn die Konfigurationssignaturen nicht übereinstimmen, werden Sie aufgefordert, die Online-Gerätekonfiguration hoch- oder die Gerätekonfiguration der Software herunterzuladen, um eine Übereinstimmung herzustellen.

Sicherheits-Reset (optional)

Wenn die Attribute des Sicherheitsgeräts auf die ursprüngliche Werkseinstellung zurückgesetzt werden sollen, verwenden Sie das Dialogfeld „Reset Safety Device“ (Sicherheitsgerät zurücksetzen).

Sie können die im Dialogfeld „Reset Safety Device“ (Sicherheitsgerät zurücksetzen) angezeigten Attribute zurücksetzen, indem Sie das entsprechende Kontrollkästchen aktivieren. Attribute, deren Kontrollkästchen nicht aktiviert werden, behalten ihre Einstellungen beim Sicherheits-Reset bei.



1. Öffnen Sie das Dialogfeld „Reset Safety Device“ (Sicherheitsgerät zurücksetzen), indem Sie in der grafischen Ansicht von RSNetWorx for DeviceNet auf das Gerät klicken und anschließend im Gerätemenü „Reset Safety Device“ (Sicherheitsgerät zurücksetzen) auswählen.

2. Prüfen Sie die zurückzusetzenden Attribute.

Attribute	Rücksetzverhalten
Konfiguration	Bei jedem Sicherheits-Reset wird die Konfiguration des Gerätes gelöscht.
Konfigurations-eigentümer	Aktivieren Sie dieses Kontrollkästchen, um den Konfigurationseigentümer des Geräts zurückzusetzen. Bei SmartGuard-Steuerungen handelt es sich beim Konfigurationseigentümer stets um die Konfigurationssoftware.
Ausgangsverbin-dungseigentümer	Aktivieren Sie dieses Kontrollkästchen, um sämtliche vorhandenen Ausgangsverbindungseigentümer zurückzusetzen. Das erste Gerät, das im Anschluss an das Sicherheits-Reset auf einen Ausgangsverbindungspunkt zugreift, wird zum Ausgangsverbindungseigentümer.
Kennwort	Aktivieren Sie dieses Kontrollkästchen, um das Gerätekennwort zurückzusetzen. Um ein Kennwort zurücksetzen zu können, muss Ihnen das aktuelle Gerätekennwort bekannt sein.
Adresse	Aktivieren Sie dieses Kontrollkästchen, um die mithilfe von Software konfigurierte Netzknotenadresse auf 63 zurückzusetzen. Wenn die Netzknotenadresse des Geräts mithilfe von Schaltern festgelegt wurde, wirkt sich das Reset nicht auf die Knotenadresse aus.
Baudrate	Aktivieren Sie dieses Kontrollkästchen, um die Kommunikationsgeschwindigkeit des Geräts auf 125 kbit/s zurückzusetzen. Wenn die Kommunikationsgeschwindigkeit des Geräts mithilfe von Schaltern fest-gelegt wurde, wirkt sich das Reset nicht auf die Kommunikationsgeschwindigkeit aus.
Sicherheitsnetz-werknummer	Aktivieren Sie dieses Kontrollkästchen, um die Sicherheitsnetzwerknummer (SNN) des Geräts zurückzusetzen.

3. Klicken Sie auf „Reset“.

Wenn die Sicherheitsverriegelung des Geräts aktiviert ist, werden Sie aufgefordert, das Gerät zunächst zu entriegeln.

ACHTUNG

Nach dem Entriegeln ist auf dem Gerät kein verlässlicher Sicherheitsbetrieb mehr möglich.

Der Betrieb des Geräts muss getestet und überprüft werden. Führen Sie zudem den Assistenten zur Überprüfung von Sicherheitsgeräten aus, um die Sicherheitsverriegelung des Geräts zu aktivieren, bevor dieses in einer Sicherheitsanwendung verwendet wird.

4. Geben Sie entsprechend der Aufforderung ein Kennwort ein, sofern für das Gerät ein solches festgelegt wurde.

Festlegen von Kennwörtern (optional)

Sie können Sicherheitsgeräte mithilfe eines Kennworts schützen, um zu verhindern, dass die Konfiguration der Geräte durch nicht autorisierte Mitarbeiter geändert wird. Wenn ein Kennwort festgelegt wurde, muss dieses bei folgenden Vorgängen eingegeben werden.

- Herunterladen
- Zurücksetzen der Sicherheitskonfiguration
- Sicherheitsverriegelung
- Sicherheitsentriegelung

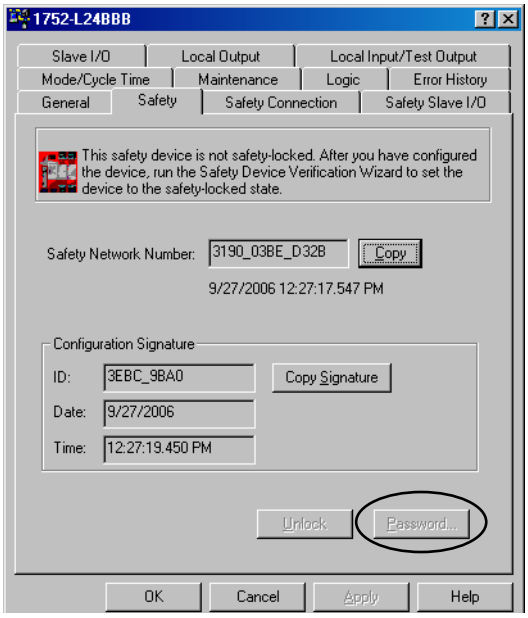
Festlegen oder Ändern von Kennwörtern

Führen Sie folgende Schritte durch, um ein Kennwort für das Modul festzulegen.

1. Doppelklicken Sie auf das Modul, um das Dialogfeld „Device Properties“ (Geräteeigenschaften) zu öffnen.

2. Wählen Sie die Registerkarte „Safety“ (Sicherheit) aus.

3. Klicken Sie auf „Password“ (Kennwort).



TIPP

Sie können auf das Dialogfeld „Set Device Password“ (Gerätekennwort festlegen) außerdem zugreifen, indem Sie:

- auf das Modul klicken und im Menü „Device“ (Gerät) die Option „Password“ (Kennwort) auswählen.
- mit der rechten Maustaste auf das Modul klicken und „Set Password“ (Kennwort festlegen) auswählen.

4. Geben Sie gegebenenfalls das alte Kennwort ein.

5. Geben Sie das neue Kennwort ein, und bestätigen Sie dieses.

   Kennwörter können zwischen einem und 40 Zeichen umfassen.
   Auf die Groß- und Kleinschreibung muss nicht geachtet werden.
   Buchstaben, Ziffern und folgende Symbole können verwendet werden:
   ‘ ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? / .

6. Klicken Sie auf „OK“.

Vergessene Kennwörter

Wenn Sie das Kennwort vergessen haben, können Sie dieses zurücksetzen.

1. Klicken Sie im Dialogfeld „Device Properties“ (Geräteeigenschaften) auf der Registerkarte „Safety“ (Sicherheit) auf „Password“ (Kennwort), um das Dialogfeld „Set Device Password“ (Gerätekennwort festlegen) zu öffnen.

2. Klicken Sie auf „Reset Password“ (Kennwort zurücksetzen).

3. Wenden Sie sich an den technischen Support von Rockwell Automation und geben Sie die Seriennummer des Geräts sowie den Sicherheitscode im Dialogfeld „Reset Password“ (Kennwort zurücksetzen) an.

4. Geben Sie im Dialogfeld „Reset Device Password“ (Gerätekennwort zurücksetzen) das vom technischen Support von Rockwell Automation erhaltene Werkskennwort ein und klicken Sie auf „OK“.

Notizen:

Einrichten Ihres EtherNet/IP-Netzwerks

Einleitung

Thema	Seite
Anschließen eines Computers an das EtherNet/IP-Netzwerk	51
Anschließen der Steuerung SmartGuard 600 an das EtherNet/IP-Netzwerk	53
Netzwerkübergreifendes Bridging	59

Anschließen eines Computers an das EtherNet/IP-Netzwerk

Führen Sie einen der folgenden Schritte aus, um auf das EtherNet/IP-Netzwerk zuzugreifen:

- Stellen Sie eine direkte Verbindung zum Netzwerk her.
- Stellen Sie eine Verbindung zu einem anderen Netzwerk her, und suchen Sie über einen Koppler nach dem gewünschten Netzwerk.

TIPP

Sie können mithilfe des USB-Anschlusses der SmartGuard-Steuerung nach dem Ethernet-Netzwerk suchen.

Die Bridging-Funktion von SmartGuard-USB zu Ethernet ist eingeschränkt.

Führen Sie im Anschluss an die Auswahl eines Netzwerks folgende Schritte durch:

- Sofern erforderlich, Installation der Kommunikationskarte.
- Ermitteln von Netzwerkparametern für den Computer, z. B. eine Netzwerkadresse.
- Anschließen des Computers am Netzwerk mithilfe des Verbindungskabels.

WICHTIG

Beim erstmaligen Anschluss einer SmartGuard-Steuerung an Ihren Computer über den USB-Anschluss führt das Betriebssystem Windows die Geräteerkennungssequenz aus. Sie werden aufgefordert, USB-Treiber anzugeben. Der Treiber befindet sich auf der RSLinx Classic-CD im Ordner „SmartGuardUSB-KernelDrivers“.

Konfigurieren des Treibers für das Netzwerk

1. Starten Sie die Software RSLinx.

   Damit die Software RSLinx neue Geräte im EtherNet/IP-Netzwerk erkennen kann, können Sie den Treiber so konfigurieren (durchsuchen Sie die dezentrale Subnetz-Option), dass er nach einer bestimmten IP-Adresse und Maske sucht.

2. Klicken Sie auf „Configure Driver“ (Treiber konfigurieren).

3. Wählen Sie im Pulldown-Menü „Available Driver Types“ (Verfügbare Treibertypen) den Treiber für Ihr Netzwerk aus.

Netzwerk	Treiber
RS-232	RS-232-DF1-Geräte
EtherNet/IP	Ethernet-Geräte
DeviceNet	EtherNet/IP-Treiber
USB	SmartGuard-USB-Treiber

4. Konfigurieren Sie den Treiber.

   Die vorzunehmenden Einstellungen sind abhängig vom ausgewählten Netzwerk und der Entscheidung, ob eine Kommunikationskarte oder ein Schnittstellenmodul verwendet werden soll.

Stellen Sie sicher, dass der Treiber funktioniert

1. Überprüfen Sie das Dialogfeld „Configure Drivers“ (Treiber konfigurieren), um sicherzustellen, dass der Treiber ausgeführt wird.

   TIPP Konfigurieren Sie den Treiber über die Option „Remote Subnet“ (Dezentrales Subnetz) und setzen Sie die IP-Adresse und Maske auf den Wert der SmartGuard-Steuerung. Auf diese Weise kann die Software RSLinx das Gerät schnell finden.

2. Schließen Sie das Dialogfeld.

3. Öffnen Sie das Dialogfeld „RSWho“.

4. Doppelklicken Sie auf den Treiber, um das Netzwerk anzuzeigen.

Anschließen der Steuerung SmartGuard 600 an das EtherNet/IP-Netzwerk

WICHTIG Die SmartGuard-Steuerungen dürfen nicht direkt an ein Netzwerk angeschlossen werden, das nicht vor Angriffen von außen geschützt ist. Schließen Sie beispielsweise die Steuerung SmartGuard 600 nicht an ein Ethernet-Netzwerk an, das nicht durch eine Firewall oder andere Sicherheitsmaßnahmen geschützt ist.

Festlegen der IP-Adresse

Definieren Sie zum Konfigurieren der Steuerung die IP-Adresse, Subnet-Maske und den Gateway.

EtherNet/IP-Parameter

EtherNet/IP-Parameter	Beschreibung
IP Address (IP-Adresse)	Die IP-Adresse dient zur eindeutigen Identifizierung der Steuerung. Die IP-Adresse wird im Format *xxx.xxx.xxx.xxx* angegeben. Dabei steht jedes *xxx* für eine Zahl zwischen 0 und 255. Die folgenden reservierten Werte können nicht verwendet werden: • 127.0.0.1 • 0.0.0.0 • 255.255.255.255
Subnet Mask (Subnet-Maske)	Die Subnetzadressierung ist eine Erweiterung des IP-Adressschemas, das die Verwendung einer einzigen Netzwerk-ID für mehrere physische Netzwerke an einem Standort erlaubt. Beim Routing außerhalb des Standorts wird die IP-Adresse über die Klasse weiterhin in eine Netz-ID und eine Host-ID unterteilt. Innerhalb eines Standorts wird die Subnet-Maske zum erneuten Unterteilen der IP-Adresse in eine benutzerdefinierte Netzwerk-ID und eine Host-ID verwendet. Dieses Feld ist standardmäßig auf 0.0.0.0 gesetzt. Wenn Sie die Subnet-Maske einer bereits konfigurierten Steuerung ändern, müssen Sie die Stromversorgung aus- und anschließend wieder einschalten, damit die Änderungen wirksam werden.
Gateway	Ein Gateway verbindet einzelne physische Netzwerke zu einem Netzwerksystem. Wenn ein Netzknoten mit einem anderen Knoten in einem anderen Netzwerk kommunizieren muss, überträgt ein Gateway die Daten zwischen den beiden Netzwerken. Dieses Feld ist standardmäßig auf 0.0.0.0 gesetzt.

Sie haben zwei Möglichkeiten, Ihre Steuerung zu konfigurieren: über die Software RSLinx Classic oder über ein BOOTP-Dienstprogramm. Informationen zur Verwendung von BOOTP finden Sie auf Seite 54, Informationen zur Verwendung der Software RSLinx finden Sie auf Seite 57.

Verwendung von BOOTP zum Festlegen der IP-Adresse

BOOTP (Bootstrap-Protokoll) ist ein einfaches Protokoll, das TCP/IP-Netzknoten verwenden, um Inbetriebnahmeinformationen zu erhalten. Eine IP-Adresse wird erst gesendet, wenn eine BOOTP-Antwort empfangen wurde. BOOTP ermöglicht es Ihnen, IP-Adressen Prozessoren im Ethernet-Verbund zuzuordnen.

Damit BOOTP verwendet werden kann, muss im lokalen Ethernet-Subnetz ein BOOTP-Server vorhanden sein. Der Server ist ein Computer, auf dem BOOTP-Server-Software installiert ist und der eine Textdatei mit Netzwerkinformationen für einzelne Netzknoten im Netzwerk liest.

Die BOOTP-Konfigurationsdatei des Hostsystems muss aktualisiert werden, um Anfragen von der SmartGuard-Steuerung verarbeiten zu können. Im Standardzustand (Auslieferungszustand) erfordert die SmartGuard-Steuerung die Verwendung eines BOOTP-Servers, um ihre IP-Adresse festlegen zu können.

Im Abschnitt Festlegen der IP-Adresse sind die zu konfigurierenden Parameter aufgeführt.

TIPP Sie können jeden beliebigen im Handel erhältlichen BOOTP-Server verwenden. Wenn Ihr Netzwerk nicht über BOOTP-Server-Fähigkeiten verfügt und Sie die SmartGuard-Steuerung dynamisch konfigurieren möchten, können Sie den kostenlosen BOOTP-Server von Rockwell Automation von folgender Adresse herunterladen http://www.rockwellautomation.com/rockwellsoftware/download/.

Wenn BOOTP aktiviert ist, treten beim Hochfahren die folgenden Ereignisse auf:

- Der Prozessor sendet eine BOOTP-Anfragenachricht, die seine Hardware-Adresse enthält, über das lokale Netzwerk oder Subnetz.
- Der BOOTP-Server vergleicht die Hardware-Adresse mit den Adressen in seiner Nachschlagetabelle.
- Der BOOTP-Server sendet eine Nachricht mit der IP-Adresse und weiteren Netzwerkinformationen, die der von ihm empfangenen Hardwareadresse entsprechen, zurück an den Prozessor.

Wenn sich die gesamte Hardware und alle IP-Adressen an einem Standort befinden, können Sie die IP-Adressen in der BOOTP-Konfigurations-File ändern, wenn Ihr Netzwerk geändert werden muss.

Die BOOTP-Anfrage kann deaktiviert werden, indem Sie die Auswahl des Parameters „BOOTP Enable“ auf der Registerkarte „Port Configuration“ (Anschlusskonfiguration) aufheben. Wenn „BOOTP Enable“ nicht ausgewählt ist (deaktiviert), verwendet die SmartGuard-Steuerung die vorhandenen Kanalkonfigurationsdaten.

WICHTIG Wenn das BOOTP-Protokoll verwendet wird, um die IP-Adresse in einer SmartGuard-Steuerung festzulegen, muss die SmartGuard-Steuerung eine anfängliche IP-Adresse vom Server empfangen, bevor das BOOTP-Protokoll deaktiviert werden kann. Es kann mithilfe der Funktion „Module Configuration" (Modulkonfiguration) in der Software RSLinx deaktiviert werden.

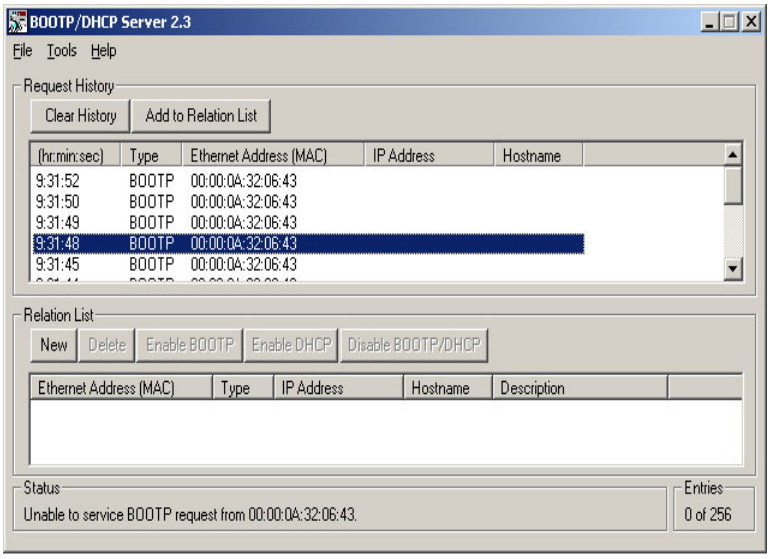
Verwendung des Rockwell BOOTP-Dienstprogramms

Das Rockwell BOOTP-Dienstprogramm ist ein eigenständiges Programm, das die Funktionalität der Standard-BOOTP-Software mit einer benutzerfreundlichen grafischen Oberfläche verbindet. Sie können es von der Adresse http://www.rockwellautomation.com/rockwellsoftware/download/ herunterladen. Auf dem Gerät muss BOOTP aktiviert sein (Werkseinstellung), damit das Dienstprogramm verwendet werden kann.

Gehen Sie zum Konfigurieren Ihres Geräts mithilfe des BOOTP-Dienstprogramms wie folgt vor.

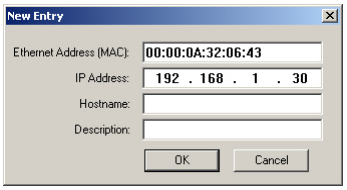
1. Starten Sie die BOOTP-Software.

   Im Fenster „BOOTP Request History" (BOOTP-Anfrageverlauf) werden die Hardware-Adressen der Geräte angezeigt, die BOOTP-Anfragen ausgeben.



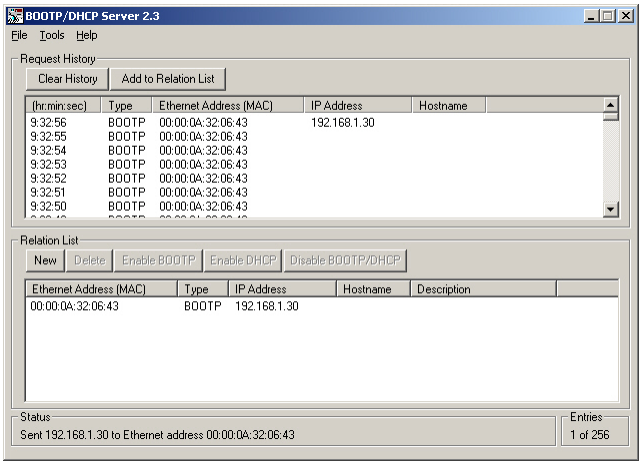
2. Doppelklicken Sie auf die Hardware-Adresse des zu konfigurierenden Geräts.

   Das Popup-Fenster „New Entry“ (Neuer Eintrag) wird mit der Ethernet-Adresse (MAC) des Geräts angezeigt.



3. Geben Sie die IP-Adresse (Hostname und Beschreibung sind optional) ein, die Sie dem Gerät zuordnen möchten, und klicken Sie auf „OK“.

   Das Gerät wird im Teilfenster „Relation List“ (Beziehungsliste) hinzugefügt. Dabei wird die Ethernet-Adresse (MAC) sowie die entsprechende IP-Adresse, Subnet-Maske und der Gateway (sofern zutreffend) angezeigt.



Verwendung der Software RSLinx zum Festlegen der IP-Adresse

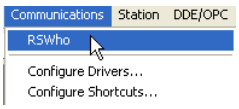
Wenn Sie das BOOTP-Dienstprogramm zum anfänglichen Festlegen der IP-Adresse einer neuen SmartGuard 600-Steuerung verwenden, können Sie anschließend die IP-Adresse mithilfe der Software RSLinx ändern. Wenn dies die von Ihnen gewünschte Funktionalität ist, müssen Sie das BOOTP-Dienstprogramm in der SmartGuard-Steuerung deaktivieren, da die SmartGuard-Steuerung sonst stets im BOOTP-Modus hochfährt.

Wenn Sie zum Konfigurieren der IP-Adressparameter in der Steuerung 1752-L24BBBE die Software RSLinx verwenden möchten, gehen Sie wie folgt vor.

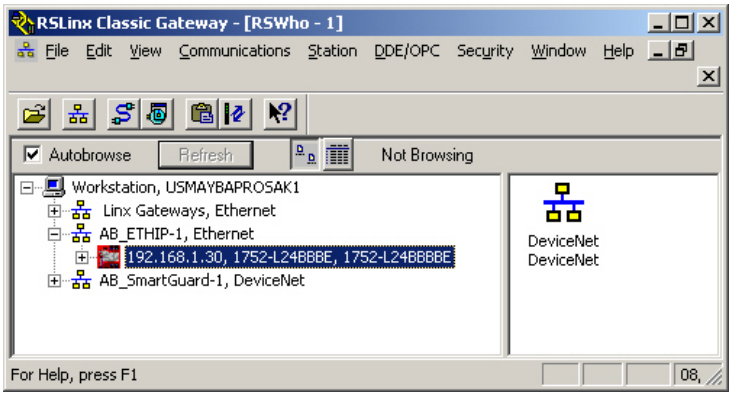
1. Stellen Sie sicher, dass die Steuerung 1752-L24BBBE installiert und eingeschaltet ist.

2. Starten Sie die Software RSLinx.

3. Wählen Sie im Pulldown-Menü „Communications“ (Kommunikation) die Option „RSWho“ aus

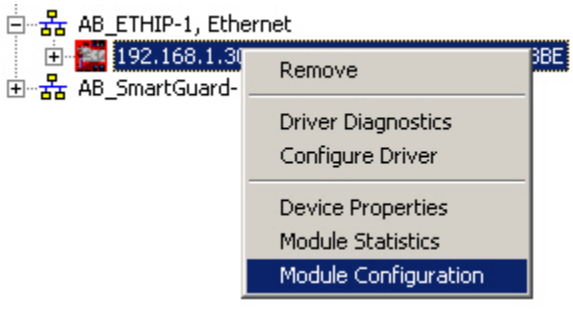


Das Dialogfeld „RSWho“ wird angezeigt.



4. Navigieren Sie in RSWho zum Ethernet-Netzwerk.

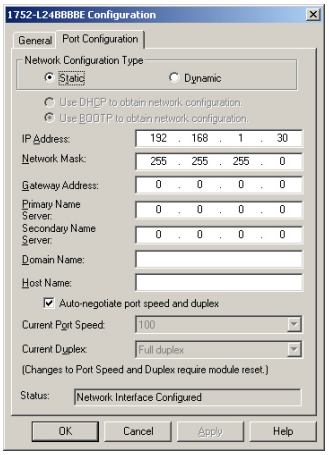
5. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung und wählen Sie „Module Configuration“ (Modulkonfiguration) aus.



TIPP

Die Option zur Modulkonfiguration wird auch angezeigt, wenn Sie die SmartGuard-Steuerung in der DeviceNet-Software ansehen, doch die IP-Konfiguration wird nur angewandt, wenn sie direkt vom EtherNet/IP-Netzwerk aus ausgeführt wird.

Das Dialogfeld „Module Configuration“ (Modulkonfiguration) wird angezeigt.



6. Klicken Sie auf die Registerkarte „Port Configuration“ (Anschlusskonfiguration).

7. Klicken Sie für „Network Configuration Type“ (Typ der Netzwerkkonfiguration) auf „Static“ (Statisch), um diese Konfiguration dem Anschluss dauerhaft zuzuordnen.

WICHTIG

Wenn Sie „Dynamic“ (Dynamisch) auswählen, löscht die Steuerung beim Aus- und Einschalten der Versorgungsspannung die aktuelle IP-Konfiguration und fährt mit dem Senden von BOOTP-Anfragen fort. Weitere Informationen finden Sie auf Seite 55.

a. Geben Sie in das Feld „IP Address“ (IP-Adresse) die IP-Adresse ein.
b. Geben Sie in das Feld „Network Mask“ (Netzwerkmaske) die Adresse der Netzwerkmaske ein.
c. Geben Sie in das Feld „Gateway Address“ (Gateway-Adresse) die Gateway-Adresse ein oder lassen Sie die Nullen unverändert.
d. Geben Sie in das Feld „Primary Name Server“ (Primärer Namensserver) die Adresse des primären Namensservers ein oder lassen Sie die Nullen unverändert.
e. Geben Sie in das Feld „Secondary Name Server“ (Sekundärer Namensserver) die Adresse des sekundären Namensservers ein oder lassen Sie die Nullen unverändert.
f. Geben Sie in das Feld „Domain Name“ (Domänenname) den Domänennamen ein oder lassen Sie das Feld leer.
g. Geben Sie in das Feld „Host Name“ (Hostname) den Namen des Hosts oder „SmartGuard ENIP“ ein.

8. Konfigurieren Sie die Anschlusseinstellungen.

Konfigurationsmethode	Vorgehensweise
Verwendung der Standardeinstellungen für Anschlussgeschwindigkeit und Duplex	Lassen Sie das Kontrollkästchen „Auto-negotiate port speed and duplex" (Automatisches Verhandeln von Anschlussgeschwindigkeit und Duplex) aktiviert. **Wichtig:** Die Standardanschlussgeschwindigkeit ist 100, die Standard-Duplex-Einstellung ist „Full" (Voll).
Manuelles Konfigurieren der Geschwindigkeits- und Duplexeinstellungen Ihres Anschlusses.	a. Deaktivieren Sie das Kontrollkästchen „Auto-negotiate port speed and duplex" (Automatisches Verhandeln von Anschlussgeschwindigkeit und Duplex). b. Wählen Sie im Pulldown-Menü „Current Port Speed" (Aktuelle Anschlussgeschwindigkeit) eine Anschlussgeschwindigkeit aus. c. Wählen Sie im Pulldown-Menü „Current Duplex" (Duplex aktuell) die Option „Half Duplex" (Halbduplex) aus.

9. Klicken Sie auf „OK".

Netzwerkübergreifendes Bridging

Die Steuerung 1752-L24BBBE unterstützt die Möglichkeit des Bridgings oder Routings von Kommunikation an verschiedene Geräte, abhängig von den Fähigkeiten der Plattform und der Kommunikationsgeräte.

Es liegt eine Bridge vor, wenn eine Verbindung zwischen den Kommunikationsgeräten auf zwei Netzwerken hergestellt wurde. Beispielsweise verfügt ein Bridge-Gerät über EtherNet/IP- und DeviceNet-Verbindungen, wobei Gerät 1 im EtherNet/IP-Netzwerk für die Kommunikation mit Gerät 2 in einem DeviceNet-Netzwerk über die Bridge aktiviert wird.

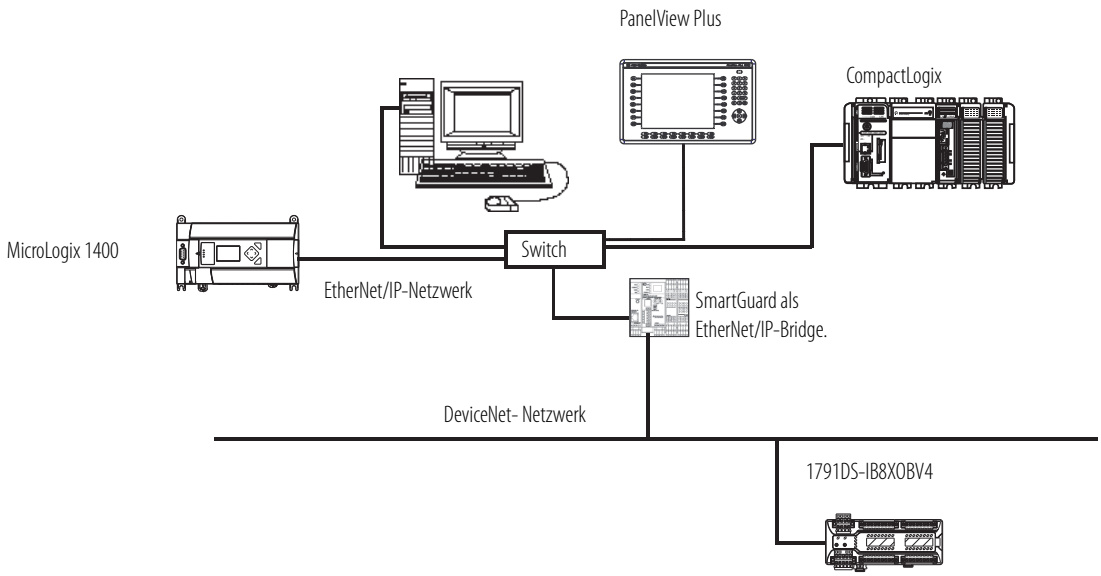
EtherNet/IP-Netzwerk zu einem DeviceNet-Netzwerk

Im Folgenden sehen Sie die Verbindung zwischen dem EtherNet/IP-Netzwerk und dem DeviceNet-Netzwerk. Die SmartGuard-Steuerung ermöglicht Ihnen die Konfiguration des 1791DS-Moduls im DeviceNet-Netzwerk mit Ihrem PC, der mit dem EtherNet/IP-Netzwerk verbunden ist, indem Sie das Bridging über die SmartGuard-Steuerung vornehmen.

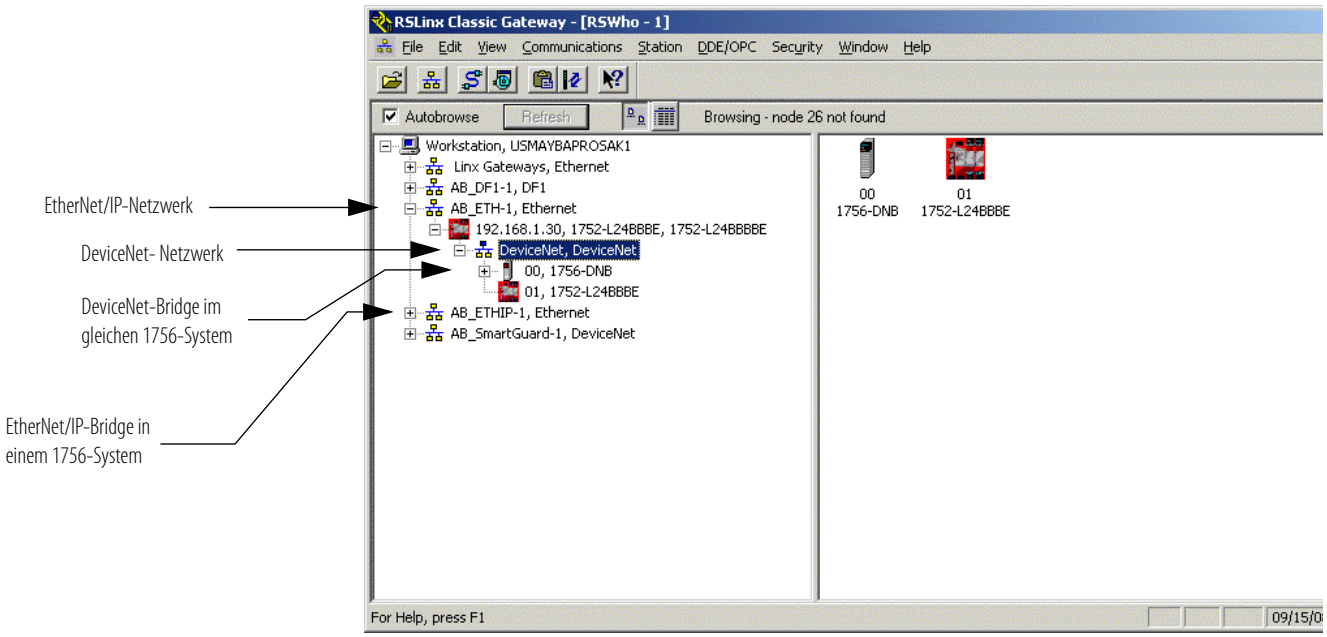
WICHTIG

Die Bridging-Funktion der SmartGuard-Steuerung ist begrenzt. Sie wurde zum Konfigurieren von Sicherheits-DIO-Modulen auf einem anderen Netzwerk entwickelt, sollte jedoch nicht zum Programmieren anderer speicherprogrammierbarer Steuerungen verwendet werden. Außerdem ist sie nicht für den Einsatz als Bridging-Gerät während des Maschinenbetriebs geeignet.

EtherNet/IP-Netzwerk zu einem DeviceNet-Netzwerk



EtherNet/IP-Bridge-Verbindung zu einem DeviceNet-Netzwerk

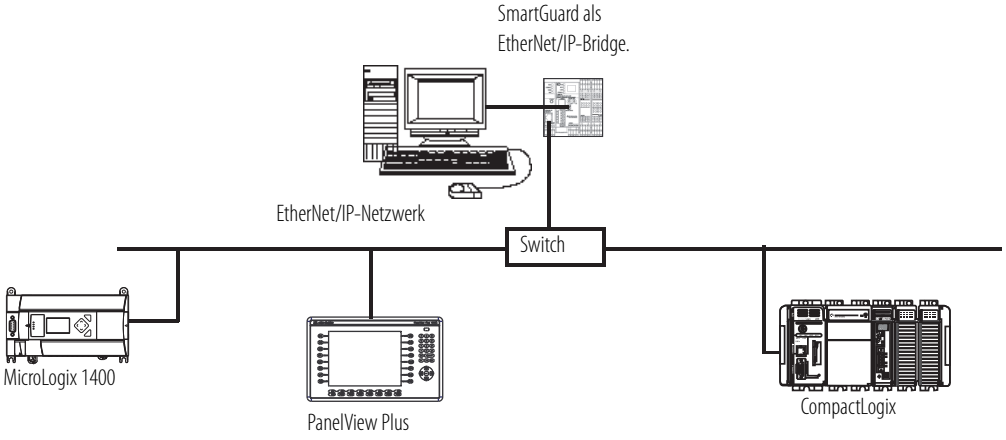


USB-Anschluss zum EtherNet/IP-Netzwerk

Die SmartGuard-Steuerung unterstützt das Bridging vom USB-Anschluss zum EtherNet/IP-Netzwerk. Allerdings wird empfohlen, diese Funktion nicht zu verwenden, sondern eine direkte Verbindung zum EtherNet/IP-Netzwerk aufzubauen, um andere Geräte außer der SmartGuard-Steuerung zu konfigurieren.

Die SmartGuard-Steuerung kann nur das Ethernet-Subnetz durchsuchen, mit dem sie verbunden ist. Sie könnten zu einer MicroLogix 1400-Steuerung oder einer CompactLogix-Steuerung wechseln, jedoch nicht zu einer ControlLogix-Steuerung, da das Routing nicht über das Modul 1756-ENBT im ControlLogix-Chassis hinaus erfolgen kann.

USB-Anschluss zum EtherNet/IP-Netzwerk



Verwalten der Sicherheitsnetzwerknummer

Einleitung

Thema	Seite
Formate der Sicherheitsnetzwerknummern (SNN)	63
Zuweisen der Sicherheitsnetzwerknummer (SNN)	65
Festlegen der Sicherheitsnetzwerknummer (SNN) in allen Sicherheitsnetzknoten	65
Abweichung der Sicherheitsnetzwerknummer (SNN)	67
Ändern der Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse	67

Alle DeviceNet Safety-Geräte müssen mit einer Sicherheitsnetzwerknummer (SNN) konfiguriert werden. Die Kombination aus SNN und der DeviceNet-Knotenadresse bietet eine eindeutige ID für jeden Sicherheitsnetzknoten in einem komplexen industriellen Netzwerk. Diese eindeutige ID verhindert, dass Daten für eine bestimmte Zielknotenadresse in einem DeviceNet-Teilnetz fälschlicherweise an einen Netzknoten weitergeleitet und von diesem akzeptiert werden, der in einem anderen Teilnetz über dieselbe Netzknotenadresse verfügt.

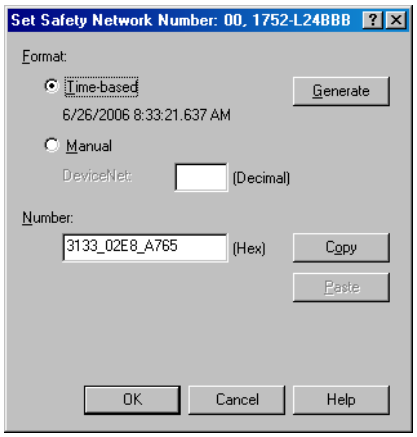
Die einem Sicherheitsnetzwerk oder Teilnetz zugeordneten Sicherheitsnetzwerknummern müssen eindeutig sein. Es muss sichergestellt werden, dass allen DeviceNet-Netzwerken mit Sicherheitsnetzknoten Sicherheitsnetzwerknummern (SNN) zugewiesen wurden.

Formate der Sicherheitsnetzwerknummern (SNN)

Die Sicherheitsnetzwerknummer (SNN) kann entweder mithilfe einer Software (zeitbasiert) oder von einem Benutzer zugewiesen werden (manuell). Diese beiden Formate der SNN werden in den folgenden Abschnitten beschrieben.

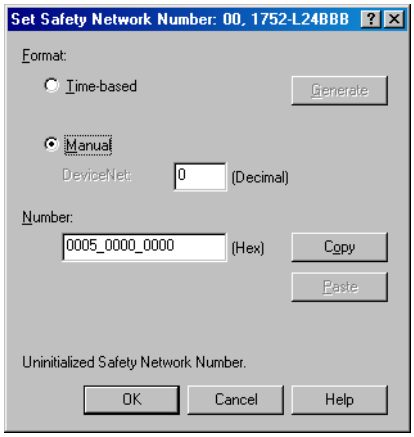
Zeitbasierte Sicherheitsnetzwerknummer (empfohlen)

Im zeitbasierten Format besteht die Sicherheitsnetzwerknummer (SNN) aus Datum und Uhrzeit der Erstellung der Nummer, entsprechend dem Computer, auf dem RSNetWorx für DeviceNet ausgeführt wird.



Manuelle Sicherheitsnetzwerknummer (SNN)

Im manuellen Format besteht die SNN aus eingegebenen Werten zwischen 1 und 9999.



TIPP

Klicken Sie im Dialogfeld „Set Safety Network Number“ (Sicherheitsnetzwerknummer festlegen) auf „Copy“ (Kopieren), um die SNN in die Windows-Zwischenablage zu kopieren.

Zuweisen der Sicherheitsnetzwerknummer (SNN)

Eine SNN kann in RSNetWorx for DeviceNet automatisch erstellt oder manuell zugewiesen werden. Für die meisten Anwendungen reicht eine automatisch erstellte SNN aus und wird daher empfohlen.

Automatisch (zeitbasiert)

Beim Hinzufügen eines neuen Sicherheitsgeräts zur Netzwerkkonfiguration wird mithilfe der Konfigurationssoftware wie folgt automatisch eine Standard-SNN zugewiesen.

- Wenn in der DeviceNet-Netzwerkkonfiguration bereits mindestens ein Sicherheitsgerät vorhanden ist, wird weiteren Sicherheitsgeräten in dieser Netzwerkkonfiguration dieselbe SNN wie die des Sicherheitsgeräts mit der niedrigsten Adresse zugewiesen.
- Wenn in der DeviceNet-Netzwerkkonfiguration keine anderen Sicherheitsgeräte vorhanden sind, wird in RSNetWorx for DeviceNet automatisch eine zeitbasierte SNN erstellt.

Manuell

Die manuelle Zuordnung eignet sich für Systeme mit einer geringen Zahl an DeviceNet-Teilnetzen und miteinander verbundenen Netzwerken, in denen die SNNs in einer für die jeweilige Anwendung logischen Form verwaltet und zugewiesen werden sollen.

WICHTIG Bei der manuellen Zuweisung einer SNN muss darauf geachtet werden, dass eine Systemerweiterung nicht zu einer Vervielfältigung von Kombinationen aus SNNs und Netzknotenadressen führt.

Um die SNN eines Sicherheitsgeräts mithilfe von RSNetWorx for DeviceNet festzulegen, wählen Sie in der grafischen Hardwareansicht das Gerät und anschließend im Menü „Device“ (Gerät) die Option „Set Safety Network Number“ (Sicherheitsnetzwerknummer festlegen) aus.

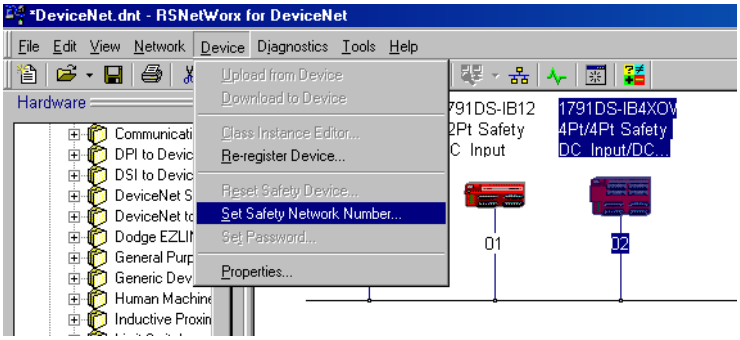
WICHTIG Beim Festlegen der SNN wird das Gerät auf die Standardwerkskonfiguration zurückgesetzt.

Festlegen der Sicherheitsnetzwerknummer (SNN) in allen Sicherheitsnetzknoten

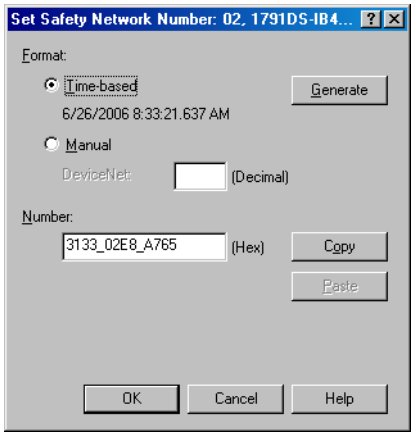
Beim Hinzufügen des ersten neuen Sicherheitsgeräts zum Netzwerk wird automatisch eine zeitbasierte SNN erstellt. Weiteren Ergänzungen des Netzwerks wird jeweils dieselbe SNN wie dem Sicherheitsgerät mit der niedrigsten Adresse zugewiesen. Für die meisten Anwendungen reicht eine automatisch erstellte zeitbasierte SNN aus und wird daher empfohlen.

Führen Sie folgende Schritte durch, wenn die SNN für ein bestimmtes Gerät festgelegt werden muss.

1. Klicken Sie in der grafischen Hardwareansicht auf das Zielgerät, und wählen Sie im Menü „Device“ (Gerät) die Option „Set Safety Network Number“ (Sicherheitsnetzwerknummer festlegen) aus.



2. Wählen Sie „Time-based“ (Zeitbasiert) aus, und klicken Sie auf „Generate“ (Generieren), oder wählen Sie „Manual“ (Manuell) aus und geben Sie eine Dezimalzahl zwischen 1 und 9999 ein.

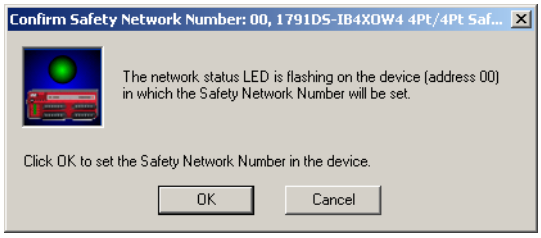


3. Klicken Sie auf „OK“.

TIPP

Sie können im Dialogfeld „Set Safety Network Number“ (Sicherheitsnetzwerknummer festlegen) die Schaltflächen für das Kopieren und Einfügen verwenden, um eine SNN zwischen Geräten zu kopieren und einzufügen und die SNN zu protokollieren.

4. Stellen Sie sicher, dass die Netzwerkstatus-LED-Anzeige am entsprechenden Gerät schnell zwischen rot und grün wechselt und klicken Sie auf „OK“.

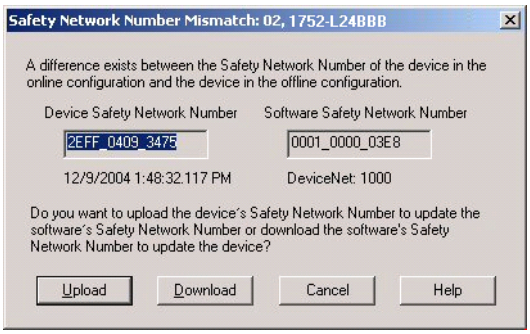


Abweichung der Sicherheitsnetzwerknummer (SNN)

In RSNetWorx for DeviceNet wird bei allen Such-, Upload- und Downloadvorgängen die Offline-SNN mit der Online-SNN abgeglichen. Dies erfolgt einmalig oder fortlaufend. Wenn die SNNs nicht übereinstimmen, wird in RSNetWorx for DeviceNet ein SNN-Fehler angezeigt. In der grafischen Hardwareansicht wird das Symbol „!“ über dem Symbol für das Sicherheitsgerät angezeigt.

Wenn RSNetWorx for DeviceNet online ist, wird immer dann auf SNN-Abweichungen geprüft, wenn das Dialogfeld „Device Properties“ (Geräteeigenschaften) entweder über das Menü „Device > Properties“ (Gerät > Eigenschaften) oder durch Doppelklicken geöffnet wird. Wenn eine SNN-Abweichung auftritt, wird das Dialogfeld „Safety Network Number Mismatch“ (Abweichung der Sicherheitsnetzwerknummer) angezeigt.

Im Dialogfeld „Safety Network Number Mismatch“ wird die Online-SNN (Gerät) und die Offline-SNN (Software) angezeigt. Um die Abweichung aufzuheben, kann entweder die SNN des Geräts hoch- oder die Offline-SNN heruntergeladen werden.



Wenn die SNN des Geräts nicht initialisiert wurde, wird im Feld „Device Safety Network Number“ (Sicherheitsnetzwerknummer des Geräts) die Standard-SNN angezeigt: FFFF_FFFF_FFFF. Wenn die SNN des Geräts „FFFF_FFFF_FFFF“ entspricht, ist die Schaltfläche „Upload“ ausgeblendet und kann nicht verwendet werden.

Ändern der Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse

Wenn die Adresse eines Sicherheitsgeräts geändert werden soll, darf die SNN nicht initialisiert sein, oder diese muss erst zurückgesetzt werden.

Führen Sie folgende Schritte durch, um die SNN zurückzusetzen.

1. Wählen Sie das Gerät in der grafischen Hardwareansicht aus.

2. Wählen Sie im Menü „Device“ (Gerät) „Reset Safety Device“ (Sicherheitsgerät zurücksetzen) aus.

3. Aktivieren Sie im Dialogfeld „Reset Safety Device“ (Sicherheitsgerät zurücksetzen) das Kontrollkästchen „Safety Network Number“ (Sicherheitsnetzwerknummer) und klicken Sie auf „Reset“ (Zurücksetzen).

   Lediglich die im Dialogfeld ausgewählten Attribute werden auf ihre Standardwerkseinstellungen zurückgesetzt. Das Sicherheits-Reset betrifft lediglich das Sicherheitsgerät. Die Konfiguration im RSNetWorx-Projekt wird beibehalten.

Weitere Informationen zur Sicherheits-Reset-Funktion finden Sie unter Sicherheits-Reset (optional) auf Seite 46.

TIPP

Im Anschluss an das Sicherheits-Reset kann die Netzknotenadresse in RSNetWorx for DeviceNet geändert werden, indem Sie in der grafischen Ansicht auf die Netzknotenadresse des Sicherheitsgeräts doppelklicken. Im Anschluss an die Änderung der Netzknotenadresse klicken Sie mit der rechten Maustaste auf das Gerät, und klicken Sie anschließend auf „Download to Device“ (Auf Gerät herunterladen), um die SNN und Konfiguration des Sicherheitsgeräts wiederherzustellen.

Konfigurieren der zentralen E/A

Einleitung

Thema	Seite
Konfigurieren der zentralen Sicherheitseingänge	69
Konfigurieren der zentralen Testausgänge	74
Konfigurieren der zentralen Sicherheitsausgänge	76

Konfigurieren der zentralen Sicherheitseingänge

Die Steuerung verfügt über 16 zentrale Sicherheitseingänge, die die folgenden Funktionen unterstützen.

- Eingangsschaltungsdiagnose – Mit Testimpulsquellen können interne Schaltungen, externe Geräte und externe Anschlüsse überwacht werden.
- Ein- und Ausschaltverzögerung des Eingangs – Sie können Eingangszeitfilter zwischen 0 und 126 ms in Vielfachen der Steuerungszykluszeit eingeben. Wenn Sie für den Eingang Ein- und Ausschaltverzögerungen festlegen, können die Auswirkungen von Rattern und externem Rauschen verringert werden.

WICHTIG

Einschalt- und Ausschaltverzögerungen für den Eingang müssen auf die E/A-Reaktionszeit aufgerechnet werden. Dies wirkt sich auch auf Reaktionszeitberechnungen für das System aus.

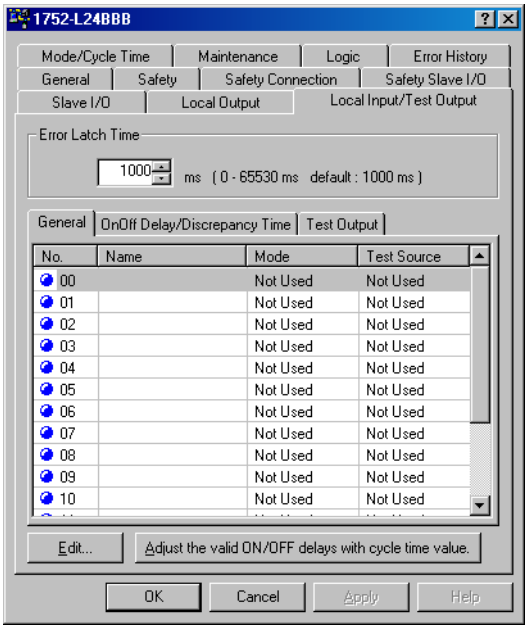
Im Sicherheitsreferenzhandbuch für die SmartGuard-Steuerungen, Publikation 1752-RM001, finden Sie Informationen zum Berechnen der Reaktionszeiten.

- Zweikanalmodus – Für Paare zusammengehöriger zentraler Eingänge können Sie den Zweikanalmodus festlegen. Wenn der Zweikanalmodus eingestellt ist, können Zeitabweichungen in den Datenänderungen oder Eingangssignalen zwischen zwei gepaarten zentralen Eingängen ausgewertet werden.

Gehen Sie zum Konfigurieren der zentralen Sicherheitseingänge folgendermaßen vor.

1. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

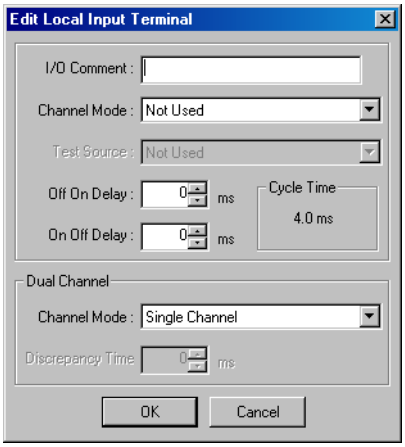
2. Wählen Sie die Registerkarte „Local Input/Test Output“ (Zentraler Eingang/Testausgang) aus.



3. Stellen Sie die Fehlerverriegelungszeit ein.

   Die Fehlerverriegelungszeit wird auf alle Sicherheitseingänge und Testausgänge angewendet. Es handelt sich um die Zeitspanne, während der der Fehlerstatus beim Auftreten eines Fehlers an einem Eingang oder Ausgang verriegelt ist. Auch wenn der Fehler behoben wird, bleibt der Fehlerstatus für die konfigurierte Fehlerverriegelungszeit stets verriegelt. Für die Fehlerverriegelungszeit können Werte von 0 bis 65 530 ms, in Schritten von 10 ms, eingestellt werden. Der Standardwert ist 1000 ms.

4. Wählen Sie eine Sicherheitseingangsklemme aus, und klicken Sie auf „Edit“ (Bearbeiten).



5. Geben Sie einen E/A-Kommentar ein.

   Der hier eingegebene E/A-Kommentar wird als E/A-Tag-Name im Logik-Editor verwendet.

6. Stellen Sie den Kanalmodus für den Sicherheitseingang ein.

Kanalmodus	Beschreibung
Nicht verwendet	Am Eingangskanal ist kein externes Gerät angeschlossen. Dies ist die Standardschaltung.
Testimpuls vom Testausgang	Verwenden Sie diesen Modus, wenn Sie eine Eingangsschaltung der Kategorie 4 aufbauen. In diesem Modus wird davon ausgegangen, dass Sie das Eingangsgerät an eine Impulstestquelle angeschlossen und anschließend mit dieser Eingangsklemme verdrahtet haben. Dies ermöglicht es, Kurzschlüsse in der Stromversorgungsleitung (positive Seite), Erdungsfehler und Kurzschlüsse in anderen Eingangssignalleitungen (Kurzschlüsse zwischen Kanälen) zu erkennen. Die Steuerung muss wissen, dass für das Eingangssignal Impulstests ausgeführt werden. Andernfalls können Fehlerauslösungen auftreten. Siehe den Abschnitt Beispiel: Eingangskanal als Testimpuls vom Testausgang auf Seite 73.
Verwendung als Sicherheitseingang	Verwenden Sie diesen Modus, wenn Sie ein Sicherheitsgerät an einen Halbleiterausgang, z. B. ein Lichtgitter, anschließen.
Verwendung als Standardeingang	Verwenden Sie diesen Modus, wenn Sie eine Verbindung zu einem Standardgerät herstellen.

7. Wenn Sie den Impulstest vom Testausgang als Kanalmodus einstellen, wählen Sie in der Dropdown-Liste „Test Source“ (Testquelle) den Testausgang aus, der zusammen mit dem Sicherheitseingang verwendet werden soll.

TIPP Der Kanalmodus des ausgewählten Testausgangs wird automatisch auf Impulstestausgang eingestellt.

8. Legen Sie den Zweikanalmodus und die Zeitabweichung fest.

Durch Festlegen des Zweikanalmodus kann der Status zweier Eingänge ausgewertet und in E/A-Tags wiedergegeben werden. Die Zeitabweichung zwischen Änderungen im Status zweier Eingänge kann ebenfalls ausgewertet werden. Die Kombinationen, die eingestellt werden können, sind bereits vordefiniert. Für die Zeitabweichung können Werte zwischen 0 und 65530 ms in Schritten von 10 ms eingestellt werden. Der Status beider Eingänge muss innerhalb der Zeitabweichung gewechselt werden. Andernfalls tritt ein Fehler auf.

Kanalmodus	Beschreibung
Einkanal	Die Sicherheitseingangsklemme wird unabhängig verwendet.
Zweikanal-Äquivalent	Die Sicherheitseingangsklemme wird als Zweikanal-Äquivalent mit einer gepaarten Sicherheitseingangsklemme verwendet.
Zweikanal-Komplement	Die Sicherheitseingangsklemme wird als Zweikanal-Komplement mit einer gepaarten Sicherheitseingangsklemme verwendet.

TIPP

Die Steuerung unterstützt Funktionsblöcke, deren Funktionen dem Zweikanalmodus gleichwertig sind. In vielen Fällen ist die Meldung und Fehlerbehebung von Systemfehlern einfacher, wenn mithilfe der Funktionsblöcke anstatt mit der SmartGuard-Hardware Fehler erkannt werden. Wenn Sie die Funktionsblöcke zum Erkennen von Systemfehlern verwenden möchten, müssen die Sicherheitseingänge für einen einzelnen Kanal konfiguriert sein.

9. Geben Sie eine Einschaltverzögerungszeit und eine Ausschaltverzögerungszeit an.

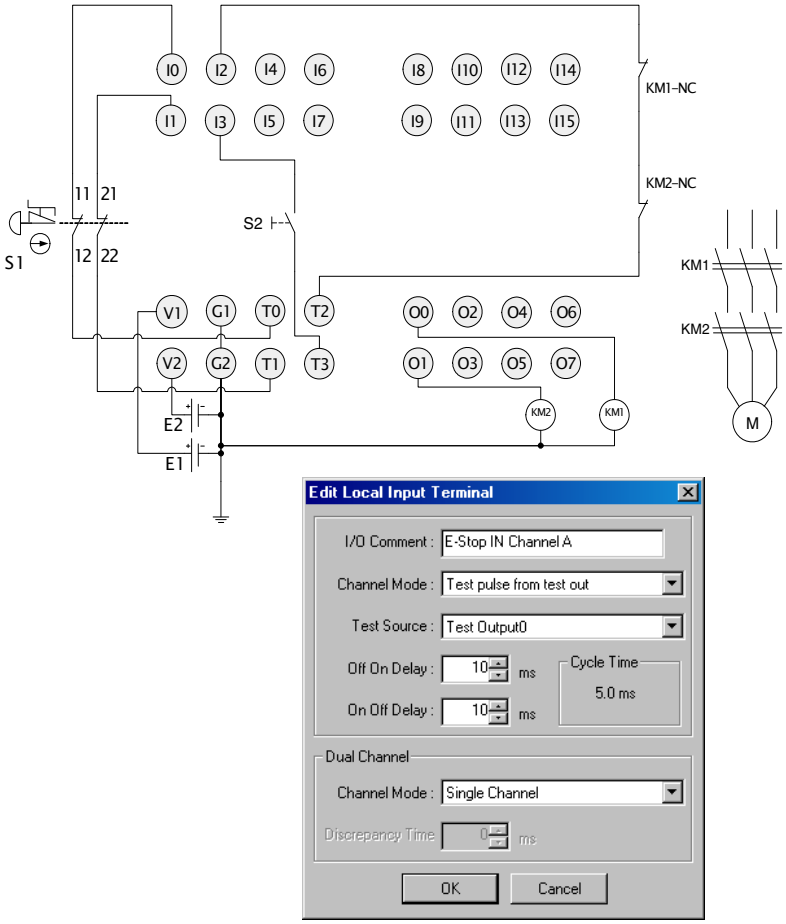
Der gültige Bereich liegt zwischen 0 und 126 ms, jedoch muss die Verzögerungszeit ein Vielfaches der Zykluszeit sein.

WICHTIG

Der optimale Wert für die Steuerungszykluszeit wird automatisch anhand der Parametereinstellungen und der Anwendungsprogramme berechnet. Stellen Sie die Ein- und Ausschaltverzögerungszeiten zuletzt ein.

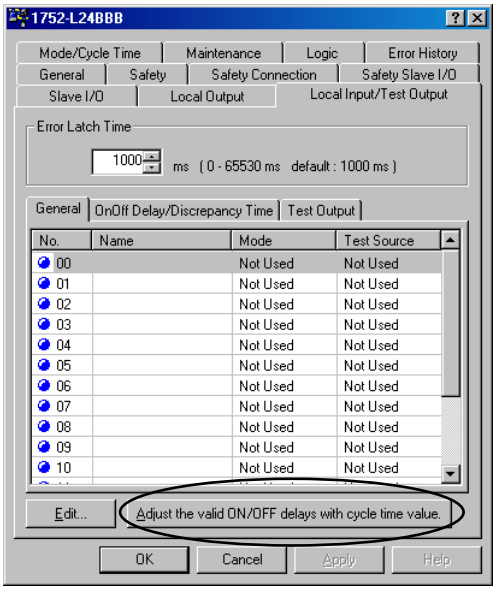
Beispiel: Eingangskanal als Testimpuls vom Testausgang

Für den folgenden Verdrahtungsplan muss der Kanalmodus wie dargestellt als Testimpuls vom Testausgang konfiguriert werden.



Automatische Anpassung von Ein- und Ausschaltverzögerungszeiten

Wenn die Zykluszeit beeinflussende Parameter nach dem Einstellen der Ein- und Ausschaltverzögerungen geändert werden, können Sie aufgrund eines Fehlers in den Parametereinstellungen möglicherweise das Dialogfeld „Controller Properties“ (Steuerungseigenschaften) nicht schließen. In diesem Fall können Sie die Ein- und Ausschaltverzögerungszeiten der Zykluszeit entsprechend neu anpassen. Verwenden Sie auf der Registerkarte „Local Input/Test Output“ (Zentraler Eingang/Testausgang) die Schaltfläche „Adjust valid ON/OFF delays with cycle time value“ (Gültige Ein-/Ausschaltverzögerungen mit Zykluszeitwert abstimmen).



Konfigurieren der zentralen Testausgänge

Diese vier voneinander unabhängigen Testausgänge können in Kombination mit Sicherheitseingängen verwendet werden. Sie können auch für die Verwendung als Standardausgangsklemmen konfiguriert werden. Im Folgenden sind die Funktionen des Testimpulsausgangs aufgeführt.

- Stromstärkeüberwachung für Muting-Lampe – Nicht angeschlossene oder durchgebrannte Glühlampen können nur an der Klemme T3 erkannt werden.
- Überstromerkennung und -schutz – Zum Schutz des Stromkreises wird ein Ausgang blockiert, sobald ein Überstrom erkannt wird.

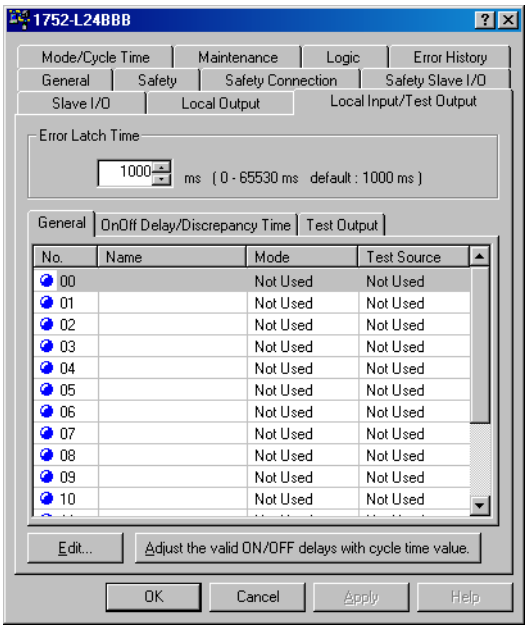
ACHTUNG

Da Impulsausgänge keine Sicherheitsausgänge sind, dürfen sie nicht in für die Sicherheit relevanten Funktionen als Ausgänge verwendet werden (zum Beispiel für die Steuerung sicherheitsrelevanter Aktoren).

Gehen Sie zum Konfigurieren eines Testausgangs folgendermaßen vor.

1. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

2. Wählen Sie die Registerkarte „Local Input/Test Output“ (Zentraler Eingang/Testausgang) aus.

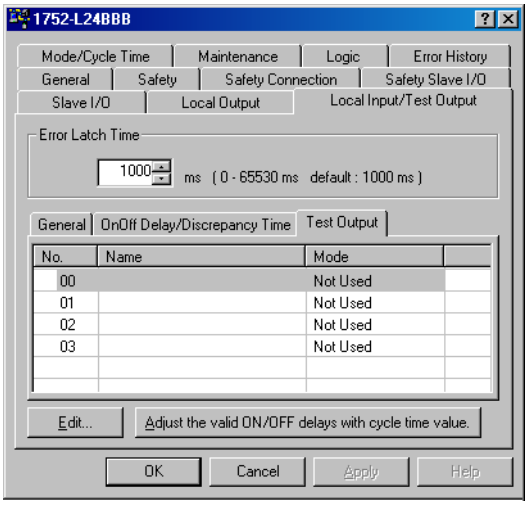


3. Stellen Sie die Fehlerverriegelungszeit ein.

   Die Fehlerverriegelungszeit wird auf alle Sicherheitseingänge und Testausgänge angewendet. Es handelt sich um die Zeitspanne, während der der Fehlerstatus beim Auftreten eines Fehlers an einem Eingang oder Ausgang verriegelt ist. Auch wenn der Fehler behoben wird, bleibt der Fehlerstatus für die konfigurierte Fehlerverriegelungszeit stets verriegelt. Für die Fehlerverriegelungszeit können Werte von 0 bis 65 530 ms, in Schritten von 10 ms, eingestellt werden. Der Standardwert ist 1000 ms.

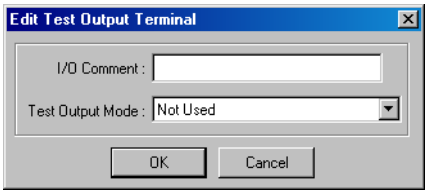
4. Wählen Sie die Registerkarte „Test Output“ (Testausgang) aus.

5. Wählen Sie eine Testausgangsklemme aus, und klicken Sie auf „Edit“ (Bearbeiten).



6. Geben Sie einen E/A-Kommentar ein.

   Der hier eingegebene E/A-Kommentar wird als E/A-Tag-Name im Logik-Editor verwendet.



7. Wählen Sie in der Dropdown-Liste einen Testausgangsmodus aus.

Testausgangsmodus	Beschreibung
Nicht verwendet	Der entsprechende Testausgang wird nicht verwendet.
Standardausgang	Wählen Sie diesen Modus, wenn Sie eine Verbindung zwischen einer Muting-Lampe oder einer programmierbaren Steuerung und dem Ausgang herstellen. Dieser Ausgang wird als Überwachungsausgang verwendet.
Impulstestausgang	Wählen Sie diesen Modus, wenn Sie ein Gerät mit einem Kontaktausgang in Kombination mit einem Sicherheitseingang verbinden.
Ausgang für Muting-Lampe	Wählen Sie diesen Modus, um einen Muting-Lampen-Ausgang anzugeben. Diese Einstellung wird nur an der Klemme T3 unterstützt. Wenn der Ausgang eingeschaltet ist, kann ein fehlender Anschluss der Muting-Lampe erkannt werden.

Konfigurieren der zentralen Sicherheitsausgänge

Die Steuerung verfügt über acht zentrale Sicherheitsausgänge, die die im Folgenden aufgeführten Funktionen unterstützen.

- Ausgangsschaltungsdiagnose – Mit Testimpulsen können Diagnosen an internen Schaltungen, externen Geräten und der externen Verdrahtung der Steuerung durchgeführt werden.
- Überstromerkennung und -schutz – Zum Schutz des Stromkreises wird ein Ausgang blockiert, sobald ein Überstrom erkannt wird.

- Zweikanalmodus – Beide Ausgänge des Paares können auf einen Sicherheitsstatus festgelegt werden, wenn an einem der paarweisen zentralen Ausgänge ohne Einfluss des Anwenderprogramms ein Fehler auftritt.

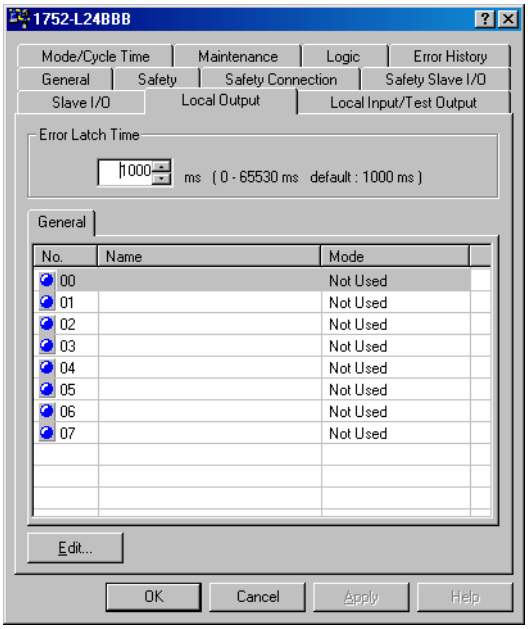
Gehen Sie zum Konfigurieren eines zentralen Sicherheitsausgangs folgendermaßen vor.

1. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

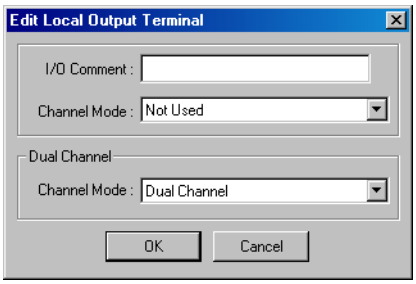
2. Wählen Sie die Registerkarte „Local Output“ (Zentraler Ausgang) aus.

3. Stellen Sie die Fehlerverriegelungszeit ein.

   Die Fehlerverriegelungszeit wird auf alle Sicherheitsausgänge angewendet. Es handelt sich um die Zeitspanne, während der der Fehlerstatus beim Auftreten eines Fehlers an einem Eingang oder Ausgang verriegelt ist. Auch wenn der Fehler behoben wird, bleibt der Fehlerstatus für die konfigurierte Fehlerverriegelungszeit stets verriegelt. Für die Fehlerverriegelungszeit können Werte von 0 bis 65 530 ms, in Schritten von 10 ms, eingestellt werden. Der Standardwert ist 1000 ms.



4. Wählen Sie eine Sicherheitsausgangsklemme aus, und klicken Sie auf „Edit“ (Bearbeiten).



5. Geben Sie einen E/A-Kommentar ein.

   Der hier eingegebene E/A-Kommentar wird als E/A-Tag-Name im Logik-Editor verwendet.

6. Stellen Sie den Kanalmodus für den Sicherheitsausgang ein.

Kanalmodus	Beschreibung
Nicht verwendet	An der Ausgangsklemme ist kein Ausgangsgerät angeschlossen.
Sicherheit	Bei eingeschaltetem Ausgang wird kein Testimpuls gesendet. Wenn der Ausgang ausgeschaltet ist, können Kurzschlüsse der Stromversorgungsleitung erkannt werden. Erdungsfehler können ebenfalls erkannt werden.
Sicherheitsimpulstest	Bei eingeschaltetem Ausgang wird ein Testimpuls gesendet. Dies ermöglicht es, Kurzschlüsse der Stromversorgungsleitung (positive Seite) sowohl bei ein- als auch bei ausgeschaltetem Ausgang zu erkennen. Zudem können Erdungsfehler und Kurzschlüsse zwischen Ausgangssignalen erkannt werden.

WICHTIG Wenn ein Sicherheitsimpulstest eingestellt ist, wird beim Einschalten des Sicherheitsausgangs ein nicht zum Impuls gehörendes Signal (Pulsweite 580 µs) gesendet, um für die Ausgangsschaltung eine Diagnose durchzuführen. Überprüfen Sie die Eingangsreaktionszeit des Steuerungsgeräts, um sich zu vergewissern, dass dieser Ausgangsimpuls keine Fehlfunktionen verursacht.

7. Stellen Sie den Zweikanalmodus für den Sicherheitsausgang ein.

   Wenn Sie den Zweikanalmodus einstellen, kann ein Fehler erkannt werden, wenn die beiden Ausgänge eines Anwenderprogramms einander nicht entsprechen. Wenn in einer der beiden Ausgangsschaltungen ein Fehler erkannt wird, werden beide Ausgänge des Geräts deaktiviert.

Einstellungen für den Zweikanalmodus des Ausgangs

Kanalmodus	Beschreibung
Einkanal	Die Sicherheitsausgangsklemme wird unabhängig verwendet.
Zweikanal	Die Sicherheitsausgangsklemme ist mit einer anderen Ausgangsklemme gepaart. Der Ausgang kann eingeschaltet werden, wenn sowohl der Ausgang als auch der paarweise Sicherheitsausgang eine Übereinstimmung bieten.

Konfigurieren der Steuerung für die DeviceNet-Kommunikation

Einleitung

Die SmartGuard-Steuerung kann gleichzeitig als Sicherheits-Master, Sicherheits-Slave oder Standard-Slave eingesetzt werden.

Thema	Seite
Konfigurieren der Steuerung als Sicherheits-Master	79
Konfigurieren der Steuerung als Sicherheits-Slave	90
Konfigurieren der Steuerung als DeviceNet-Standard-Slave	98
Lesen und Schreiben von der und auf die SmartGuard-Steuerung zu einer PanelView Plus-Schnittstelle	103

Konfigurieren der Steuerung als Sicherheits-Master

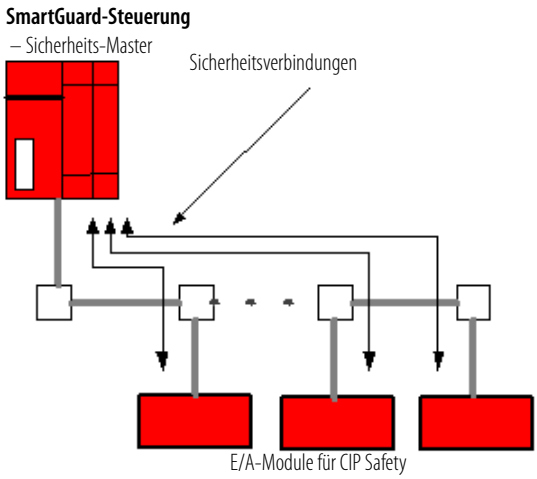
Als Sicherheits-Master kann die Steuerung E/A-Sicherheits-Kommunikationsvorgänge mit bis zu 32 Verbindungen und 16 Byte pro Verbindung durchführen. Es können Singlecast- oder Multicast-Verbindungen verwendet werden.

Die unterschiedlichen Typen verteilter E/A-Sicherheitsmodule belegen unterschiedlich viele der 32 verfügbaren Verbindungen. Zum Beispiel belegt ein reines Eingangsmodul normalerweise 1 der 32 Verbindungen (Eingangsverbindung), während ein Modul mit Ein- und Ausgängen normalerweise 2 der 32 Sicherheitsverbindungen belegt (1 Eingangsverbindung und 1 Ausgangsverbindung).

Mit der Konfiguration des Moduls wird auch die Anzahl der von diesem belegten Sicherheitsverbindungen vorgegeben. Beispielsweise belegt das Modul 1791DS-IB12 12 Sicherheitseingänge, keine Sicherheitsausgänge sowie 4 Standard- oder Impulstestausgänge. Wenn dieses Modul nur für Sicherheitseingänge konfiguriert wird, belegt es 1 Sicherheitsverbindung. Wenn das Modul jedoch für die Verwendung von Sicherheitseingängen und Standardausgängen konfiguriert wird, belegt es 2 Sicherheitsverbindungen. Letztlich bestimmen die Anzahl und der Typ der verteilten, an die SmartGuard-Steuerung angeschlossenen E/A-Sicherheitsmodule die maximale Anzahl der Module, die von der Steuerung gesteuert werden können.

Für jede Verbindung im DeviceNet-Sicherheitsnetzwerk wird eine Master/Slave-Beziehung eingerichtet, die von der Master/Slave-Kommunikation im DeviceNet-Standardnetzwerk getrennt ist. Dies ermöglicht es der Steuerung, die als Sicherheits-Master fungiert, die Sicherheitsverbindungen zu steuern.

SmartGuard-Steuerung als Sicherheits-Master

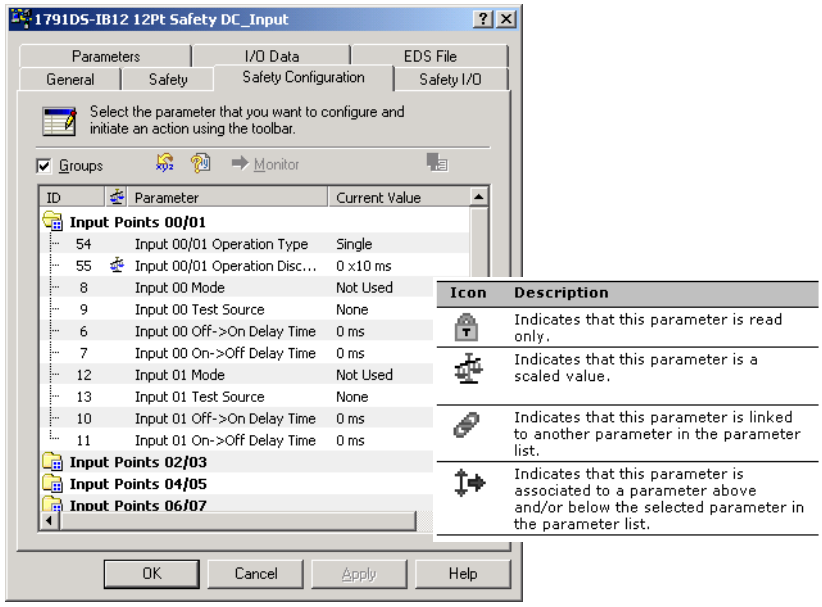


Konfigurieren von E/A-Zielen für CIP Safety im DeviceNet-Netzwerk

Um das Modul zu konfigurieren, doppelklicken Sie in der grafischen Ansicht auf das Modul oder klicken Sie mit der rechten Maustaste auf das Modul und wählen Sie „Properties“ (Eigenschaften) aus.

Sicherheitseingangs-, Sicherheitsausgangs- und Test-Parameter

Sicherheitsparameter werden im Dialogfeld „Module Properties“ (Moduleigenschaften) auf der Registerkarte „Safety Configuration“ (Sicherheitskonfiguration) konfiguriert.



Vergleich zwischen Einkanal und Zweikanal-Äquivalent oder Zweikanal-Komplement

Sie können dezentrale E/A-Moduleingänge für den Ein- oder Zweikanalmodus verwenden. Auf diese Weise wird das Guard I/O-Modul darüber informiert, ob die Eingänge einzeln (Einkanal) oder als Eingangspaare (Zweikanal) angezeigt werden sollen. Zweikanaleingänge können als äquivalent konfiguriert werden, wobei beide Eingänge stets identisch oder komplementär sein sollten (als Komplement sollten sich beide Eingänge stets gegenüberliegen).

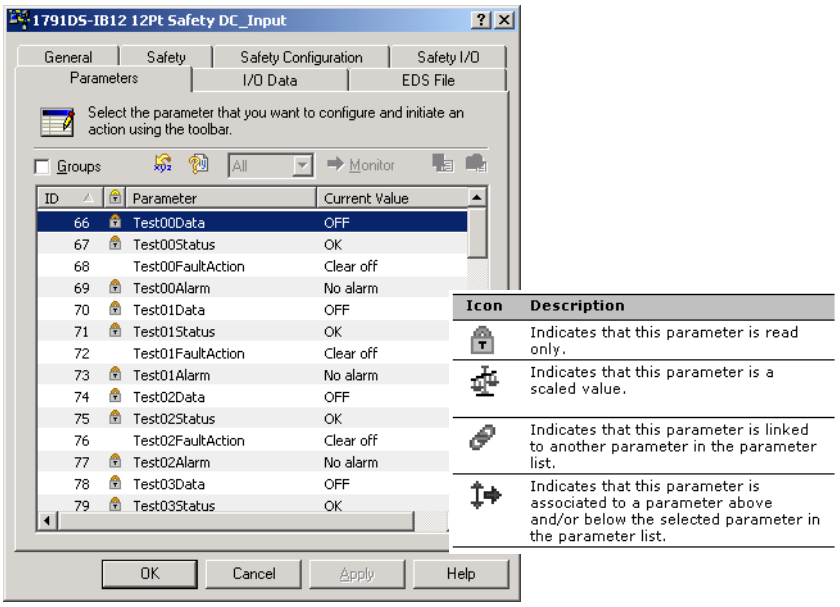
Sofern als zweikanalig konfiguriert, sendet das Guard I/O-Modul stets die Kanaldaten an die SmartGuard-Steuerung, wobei beide Kanäle deaktiviert (LO) oder aktiviert (HI) sind. Dies bedeutet dass der Fehler „Inputs Inconsistent“ (Eingänge inkonsistent) mit dem SmartGuard-Befehl nie auftritt.

Wenn der SmartGuard-Befehl die Diagnose des Sicherheitseingangs an den Guard I/O-Modulen ausführen soll, konfigurieren Sie die Guard I/O-Module als einen Kanal. Auf diese Weise können Sie die Fehleranzeigen verwenden, die vom SmartGuard-Befehl in Ihrem Programm zur Verfügung gestellt werden (empfohlen).

Wenn Sie die Diagnose des Sicherheitseingangs am Guard I/O-Modul mit den Modulstatusanzeigen und Status-Bits ausführen möchten und nicht mithilfe der SmartGuard-Befehlsdiagnose, konfigurieren Sie das Guard I/O-Modul als zweikanalig-komplementär oder äquivalent.

Standard-Eingangs- und Ausgangsparameter

Die hier gezeigten Module vom Typ 1791DS unterstützen sowohl Standarddaten als auch Sicherheitsdaten. Konfigurieren Sie die Standard-Eingangs- und Ausgangsparameter im Dialogfeld „Module Properties“ (Moduleigenschaften) auf der Registerkarte „Parameters“ (Parameter).



TIPP Auf anderen Geräten stehen möglicherweise andere Konfigurationsoptionen zur Verfügung. Weitere Informationen finden Sie im Benutzerhandbuch für das betreffende Gerät.

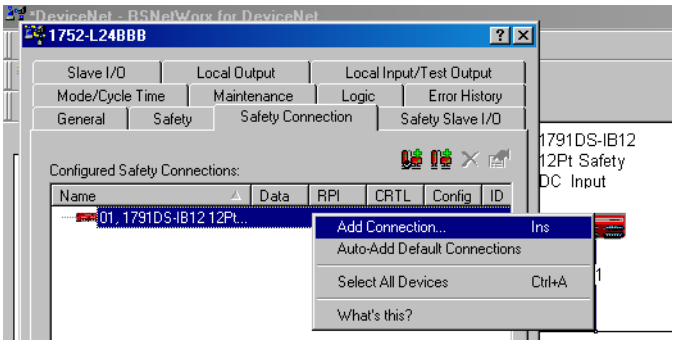
Herunterladen der Gerätekonfigurationen

Sobald Sie die Sicherheits- und Standardparameter des E/A-Moduls konfiguriert haben, laden Sie die Konfiguration auf die Module herunter. Wählen Sie hierfür in der Software RSNetWorx for DeviceNet im Menü „Device“ (Gerät) die Option „Download to Device“ (Auf Gerät herunterladen) aus.

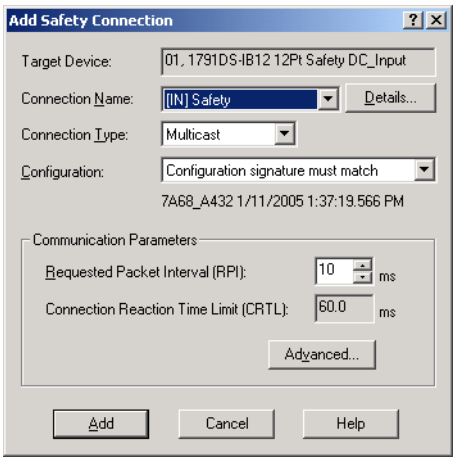
Konfigurieren von E/A-Sicherheitsverbindungen

E/A-Sicherheitsverbindungen werden für den automatischen Datenaustausch mit den Sicherheits-Slaves ohne Anwenderprogrammierung verwendet. Für die E/A-Sicherheitskommunikation mit anderen Slaves müssen Sie die Verbindung mit der SmartGuard-Steuerung konfigurieren.

1. Klicken Sie auf der Registerkarte „Safety Connections“ (Sicherheitsverbindungen) mit der rechten Maustaste auf das E/A-Modul, und wählen Sie „Add Connections“ (Verbindungen hinzufügen) aus, um alle verfügbaren Verbindungen anzuzeigen.



   Im Dialogfeld „Add Safety Connection“ (Sicherheitsverbindungen) können Sie eine Verbindung konfigurieren.



2. Wählen Sie die gewünschte Verbindung über den Verbindungsnamen aus.

3. Wählen Sie einen Verbindungstyp aus, d. h. Multicast (nur Eingangsverbindungen) oder Punkt-zu-Punkt (Eingangs- oder Ausgangsverbindungen).

4. Wählen Sie „Configuration signature must match“ (Übereinstimmung der Konfigurationssignatur erforderlich) aus.

Mit dieser Auswahl wird die SmartGuard-Steuerung die Konfigurationssignatur beim Herstellen einer Verbindung mit dem E/A-Modul berücksichtigen und das E/A-Modul wird die Verbindung nur akzeptieren, wenn die Signatur mit der im Gerät übereinstimmt.

WICHTIG Wenn Sie nicht „Configuration signature must match" (Übereinstimmung der Konfigurationssignatur erforderlich) auswählen, müssen Sie die Sicherheitsintegrität des Systems auf andere Weise selbst überprüfen.

5. Überprüfen Sie die Reaktionszeitgrenze der Verbindung.

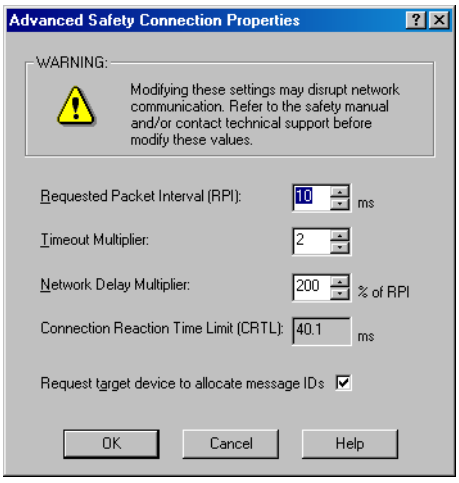
   Die Reaktionszeitgrenze der Verbindung ist das maximale Alter der Sicherheitspakete auf der zugehörigen Verbindung. Falls das Alter der vom konsumierenden Gerät verwendeten Daten die Reaktionszeitgrenze der Verbindung überschreitet, tritt ein Verbindungsfehler auf. Passen Sie die Reaktionszeitgrenze der Verbindung an, indem Sie das angeforderte Paketintervall (RPI) oder die erweiterten Kommunikationseigenschaften wie in den Schritten 6 und 7 beschrieben ändern.

6. Legen Sie das angeforderte Paketintervall (RPI) fest.

   Das RPI gibt das Zeitintervall an, in dem Daten über eine Verbindung aktualisiert werden. Das RPI wird in Schritten von 1 ms eingegeben. Die Steuerung unterstützt einen gültigen Bereich von 5 bis 500 ms, wobei der Standardwert bei 10 ms liegt. Die RPI-Bereiche anderer Zielgeräte sind möglicherweise stärker eingeschränkt. In der Dokumentation des jeweiligen Zielgerättyps finden Sie Informationen zum unterstützen Bereich und zu den Inkrementalwerten.

   Änderungen des RPI wirken sich auf die Reaktionszeitgrenze der Verbindung aus. Für einfache Zeitmessungsanforderungen ist das Festlegen des RPI normalerweise ausreichend. Bei komplexeren Anforderungen klicken Sie jedoch auf „Advanced" (Erweitert), um die Zeitwerte, die sich auf die Reaktionszeitgrenze der Verbindung auswirken, weiter anzupassen.

7. Legen Sie die erweiterten Eigenschaften von Sicherheitsverbindungen fest (bei Bedarf).



- Timeout-Multiplikator – Der Timeout-Multiplikator bestimmt die Anzahl von RPIs, die gewartet wird, bevor ein Verbindungs-Timeout ausgegeben wird. Dies lässt sich durch die Anzahl der Nachrichten ausdrücken, die verloren gehen können, bevor ein Verbindungsfehler ausgewiesen wird. Ein Timeout-Multiplikator von 1 zeigt beispielsweise an, dass Nachrichten während jedes RPI-Intervalls empfangen werden müssen. Ein Timeout-Multiplikator von 2 gibt an, dass 1 Meldung verloren gehen kann, solange mindestens 1 Meldung innerhalb des doppelten RPI (2 x RPI) empfangen wird.
- Netzwerkverzögerungs-Multiplikator – Der Netzwerkverzögerungs-Multiplikator definiert die vom Kommunikationsprotokoll erzwungene Meldungstransportzeit. Der Netzwerkverzögerungs-Multiplikator spezifiziert die Verzögerung durch die Übertragung vom Producer zum Consumer und zurück zum Producer. Sie können den Netzwerkverzögerungs-Multiplikator verwenden, um die Reaktionszeitgrenze der Verbindung zu verringern oder zu erhöhen, wenn die erzwungene Meldungtransportzeit wesentlich kürzer oder länger als das RPI ist.

8. Wählen Sie im Menü „File“ (Datei) die Option „Save“ (Speichern) aus, um Ihre Konfiguration zu speichern.

Ändern einer E/A-Verbindung

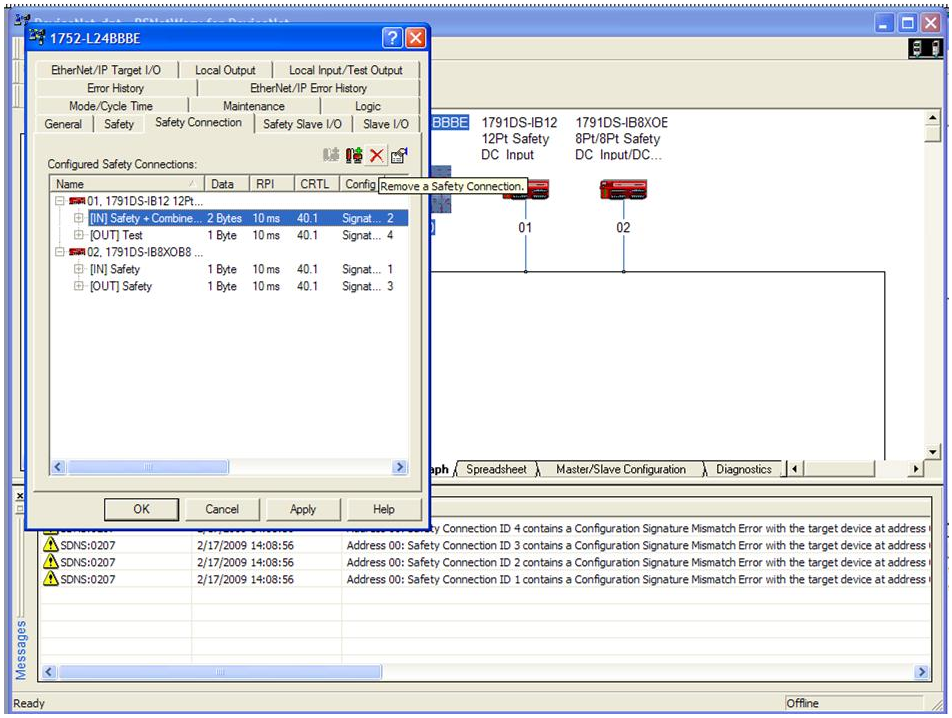
ACHTUNG

Wenn Logik mithilfe dezentraler E/A-Module (DIO) und der SmartGuard-Steuerung programmiert wird und Sie eine sichere Verbindung zu einem DIO-Modul löschen (oder löschen und erneut hinzufügen), werden die dezentralen E/A-Verbindungen im Logikeditor als ungültig markiert und könnten in den falschen Funktionsblock verschoben werden. Das Herunterladen ist erst möglich, wenn diese Fehler behoben wurden.

Wenn Sie eine Verbindung zu einem DIO-Modul löschen, nachdem die Logik geschrieben wurde, müssen Sie zur Logik zurückkehren und die Tags in Ihrem Programm verifizieren oder an die richtigen Funktionsblöcke anpassen. Notieren Sie die Sicherheitsverbindungen und -zuordnungen, bevor Sie die Verbindungen löschen oder wiederherstellen. Überprüfen Sie diese Verbindungen, bevor Sie die Logik in Ihrer Anwendung ausführen.

Gehen Sie wie folgt vor, um Ihre Sicherheitsverbindungen zu ändern.

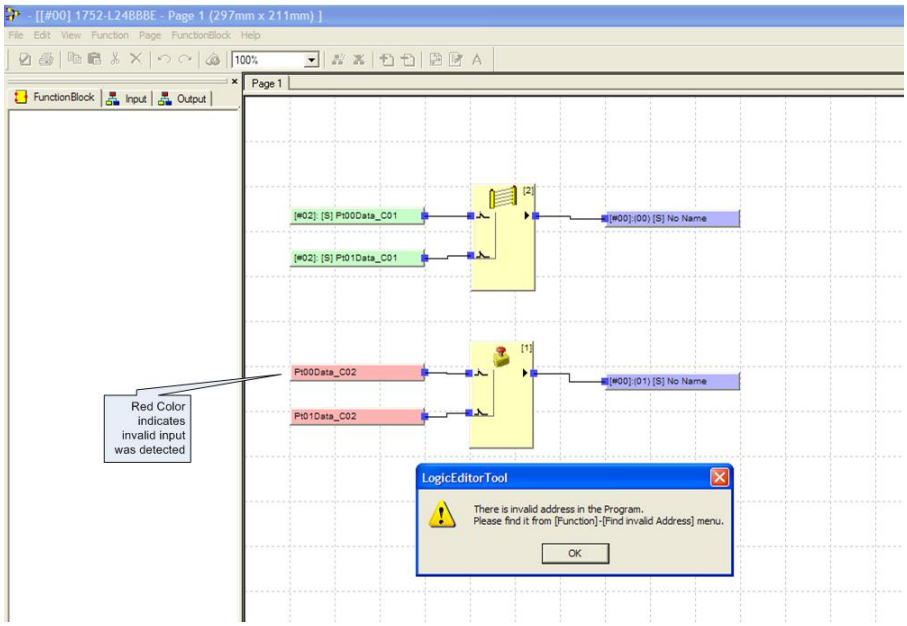
1. Heben Sie die E/A-Verbindung hervor, die Sie ändern oder entfernen möchten.



2. Klicken Sie auf die Schaltfläche „x“.

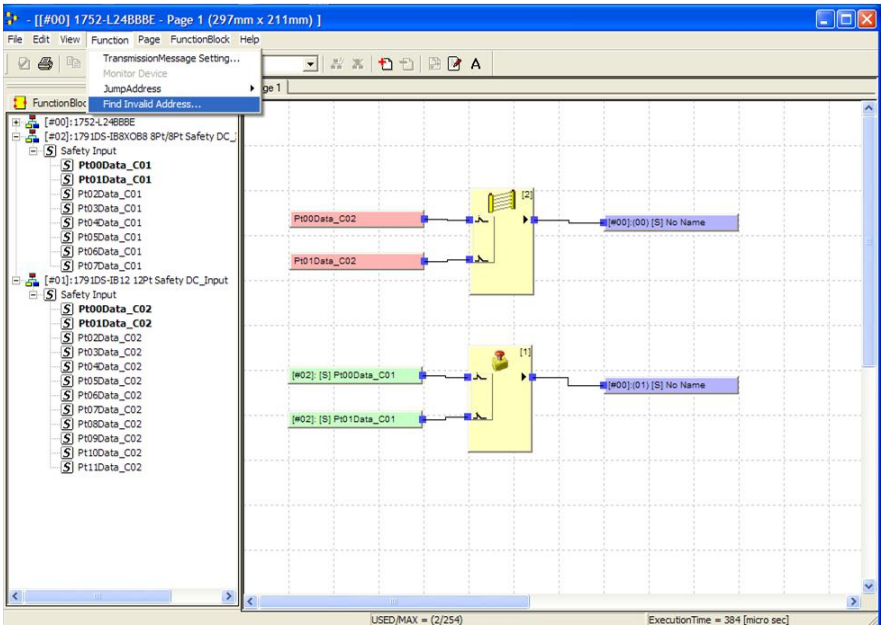
   Dies ermöglicht das Entfernen einer E/A-Verbindung.

Wenn Sie Ihre Logik in diesem Beispiel das nächste Mal ansehen, wird ein Dialogfeld mit einer Fehlermeldung angezeigt.

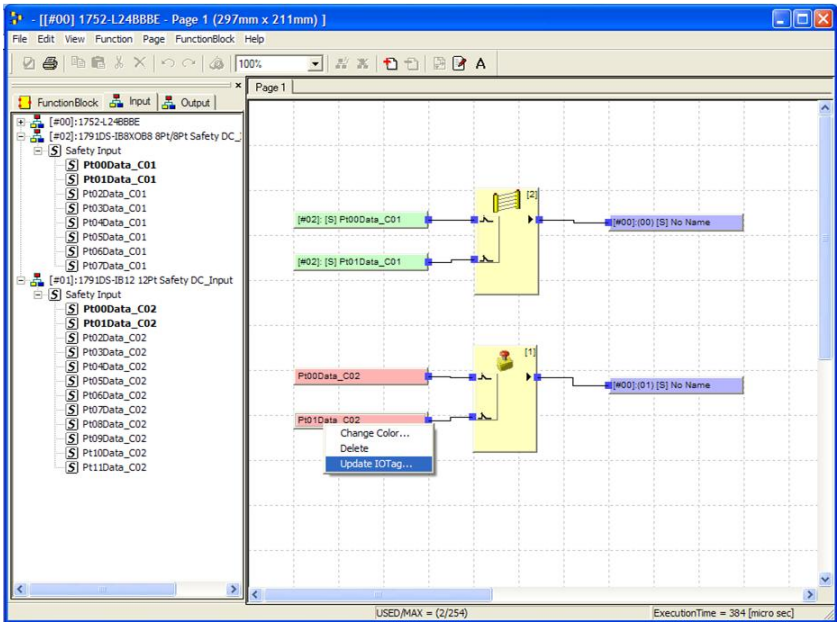


3. Klicken Sie auf „OK“.

4. Wählen Sie zum Suchen ungültiger Adressen die Optionen „Function>Find Invalid Address“ (Funktion>Ungültige Adresse suchen) aus oder suchen Sie nach rot markierten E/A-Tags und klicken Sie mit der rechten Maustaste auf das rot markierte E/A-Tag.



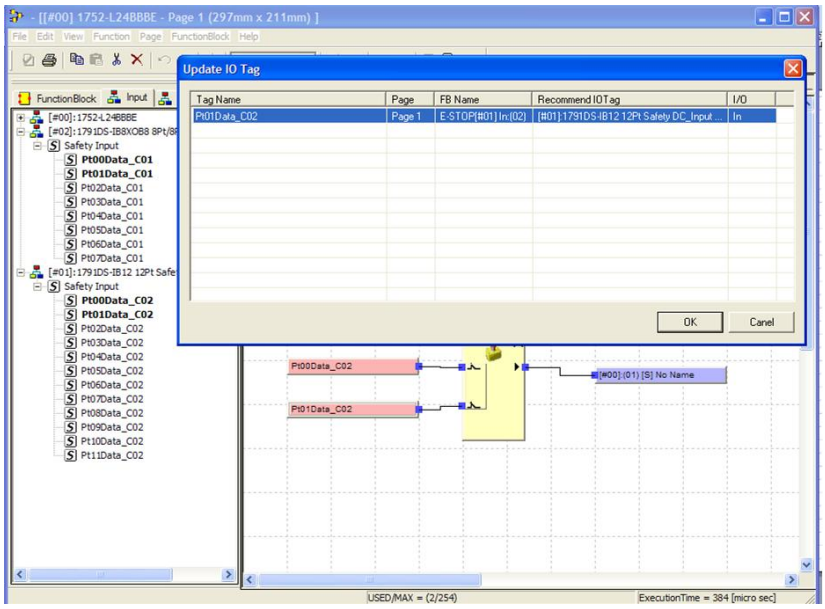
Auf dem ungültigen Tag wird ein Pulldown-Menü angezeigt.



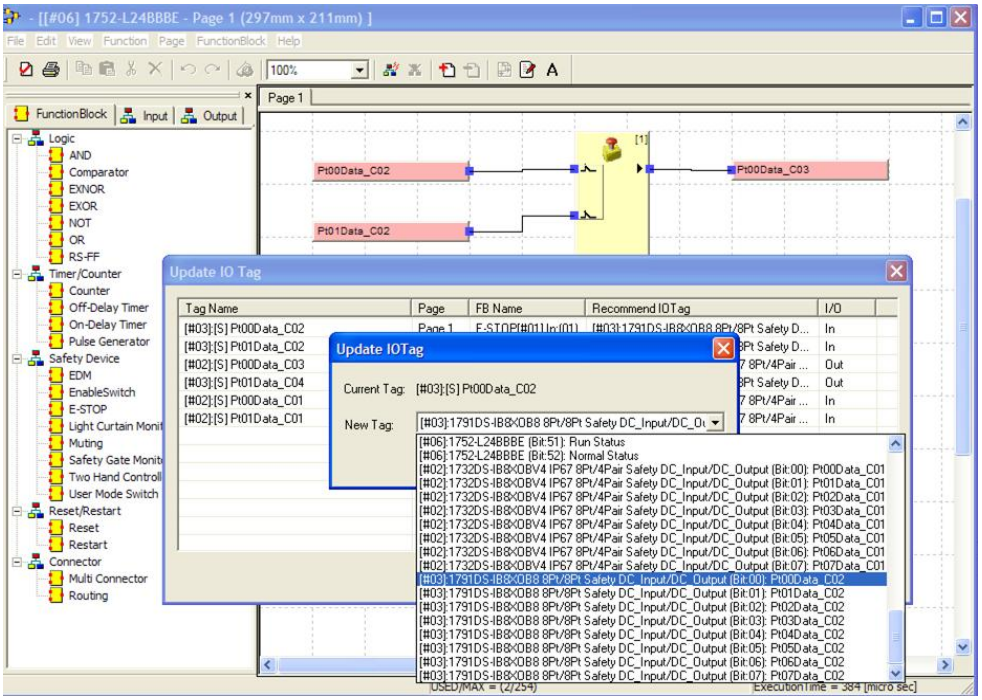
5. Klicken Sie mit der rechten Maustaste auf das ungültige Tag.

   Das Pulldown-Menü „Update IO Tag“ (E/A-Tag aktualisieren) wird angezeigt.

   Im Dialogfeld wird der Tag-Fehler mit dem empfohlenen Tag angezeigt. Das empfohlene Tag ist ein Vorschlag der Software im Hinblick darauf, mit welchem E/A-Punkt das Tag ursprünglich verbunden war. Doch Sie müssen dies durch Doppelklicken auf die vorgeschlagene Option überprüfen und bestätigen.



6. Wenn das empfohlene Tag korrekt ist, heben Sie das Tag hervor,und klicken Sie auf „OK“. Wenn das empfohlene Tag nicht korrekt ist, doppelklicken Sie auf die Linie. Es wird ein neues Dialogfeld angezeigt, in dem Sie ein Ersatz-Tag auswählen können. Wenn Sie nach unten blättern, werden weitere Optionen angezeigt.



7. Klicken Sie auf „OK“.

ACHTUNG

Wenn im Dialogfeld „Update I/O Tag“ (E/A-Tag aktualisieren) mehrere Tags angezeigt werden, müssen Sie alle Tags akzeptieren oder Alternativen auswählen, bevor Sie auf „OK“ klicken. Anderenfalls wird das empfohlene E/A-Tag verwendet.

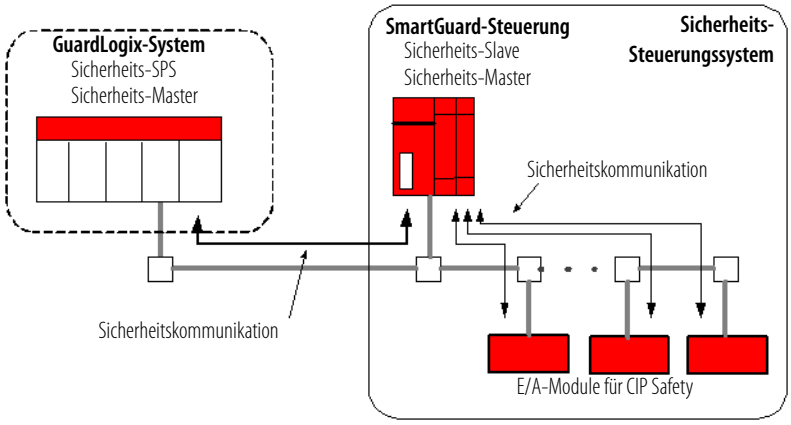
Empfehlungen zum Konfigurieren Ihres Sicherheitssystems finden Sie im Sicherheitsreferenzhandbuch für die SmartGuard 600-Steuerungen, Publikation 1752-RM001.

Konfigurieren der Steuerung als Sicherheits-Slave

Als Sicherheits-Slave kann die Steuerung E/A-Sicherheits-Kommunikationsvorgänge mit bis zu 4 Verbindungen und 16 Byte pro Verbindung durchführen. Dabei können Singlecast- oder Multicast-Verbindungen verwendet werden. Bei einer einzelnen Multicast-Verbindung liegt die Gesamtzahl der Master, mit denen kommuniziert werden kann, jedoch bei 15.

Wenn die SmartGuard-Steuerung E/A-Sicherheitskommunikationsvorgänge als Sicherheits-Slave ausführen soll, müssen Sicherheits-Slave-E/A-Daten erstellt und E/A-Sicherheitsverbindungen auf dem Sicherheits-Master konfiguriert werden.

SmartGuard-Steuerung als Sicherheits-Slave und Sicherheits-Master



Wenn die Steuerung als Sicherheits-Slave betrieben wird, können Sie die Sicherheits-Slave-Baugruppen für die Übertragung von zentralen E/A-Daten (Überwachungsdaten), Steuerungs- und E/A-Statusdaten sowie verteilten E/A-Daten an einen Sicherheits-Master konfigurieren. Der Sicherheits-Master kann auch Sicherheitsdaten an die SmartGuard-Slave-Steuerung schreiben, die von dieser im eigenen Anwendungsprogramm verwendet werden können.

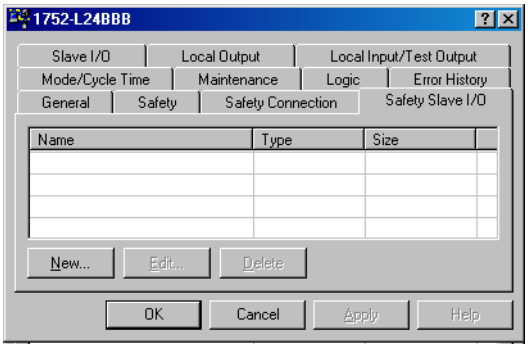
Wenn Statusdaten festgelegt sind, wird der Status am Anfang des dezentralen E/A-Bereichs zugeordnet, wobei die Statusdaten den zentralen E/A-Daten vorangestellt sind. Anschließend folgen vom Anwender registrierte E/A-Tags. Nicht festgelegte Statusbereiche werden nicht reserviert. Gültige Daten werden keinesfalls nicht zugewiesenen Bereichen zugeordnet.

Erstellen von Sicherheits-Slave-E/A-Daten

Gehen Sie folgendermaßen vor, um eine Sicherheits-Slave-Baugruppe zu erstellen.

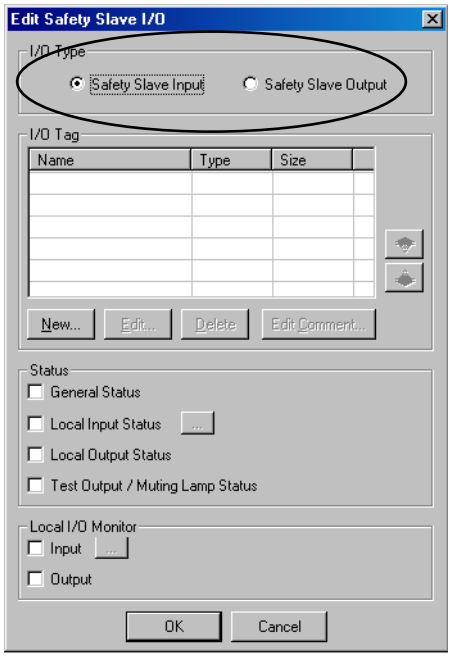
1. Klicken Sie in RSNetWorx for DeviceNet mit der rechten Maustaste auf die SmartGuard-Steuerung, die als Sicherheits-Slave eingesetzt werden soll, und wählen Sie dann „Properties“ (Eigenschaften) aus.

2. Klicken Sie auf die Registerkarte „Safety Slave I/O“ (Sicherheits-Slave-E/A).



3. Klicken Sie auf „New“ (Neu).

4. Klicken Sie im Dialogfeld „Edit Safety Slave I/O“ (Sicherheits-Slave-E/A bearbeiten) auf den E/A-Typ: entweder „Safety Slave Input“ (Safety-Slave-Eingang) oder „Safety Slave Output“ (Safety-Slave-Ausgang).



E/A-Typ	Richtung der Sicherheitsdaten
Safety Slave Input	Sicherheits-Slave der SmartGuard-Steuerung —> Sicherheits-Master
Safety Slave Output	Sicherheits-Master —> Sicherheits-Slave der SmartGuard-Steuerung

5. Aktivieren Sie zum Hinzufügen von Statusinformationen für Sicherheitseingangstypen das entsprechende Kontrollkästchen im Bereich „Status“.

Tag-Name	Datengröße	Attributtyp
Allgemeiner Status	Byte	Standard

Tag-Name	Datengröße	Attributtyp
Status zentraler Eingang	Wort	Sicherheit
Status zentraler Ausgang	Byte	Sicherheit
Status Testausgang/Muting-Lampe	Byte	Standard

Sicherheitsausgangstypen dürfen keine Statusdaten enthalten. Statusdaten können nur gelesen und nicht geschrieben werden.

6. Zum Hinzufügen zentraler E/A-Überwachungsdaten für Eingangstypen überprüfen Sie das entsprechende Kontrollkästchen im Bereich „Local I/O Monitor“ (Zentrale E/A-Überwachung).

Tag-Name	Datengröße	Attributtyp
Überwachung zentraler Eingang 1 (Eingänge 0 bis 7)	Byte	Sicherheit
Überwachung zentraler Eingang 2 (Eingänge 8 bis 15)	Byte	Sicherheit
Überwachung zentraler Ausgang (Ausgänge 0 bis 7)	Byte	Sicherheit

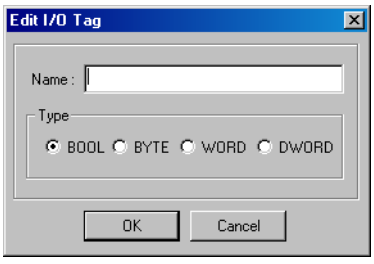
Sicherheitsausgangstypen dürfen keine zentralen E/A-Überwachungsdaten enthalten. Eingangs- und Ausgangswerte können nur gelesen und nicht direkt geschrieben werden.

7. Klicken Sie auf „New“ (Neu), um ein E/A-Tag für die Sicherheitsbaugruppe zu erstellen.

   In einer E/A-Baugruppe können mehrere E/A-Tags definiert werden. In jeder E/A-Baugruppe können E/A-Tags für bis zu 16 Bytes definiert werden. Die dort definierten E/A-Tags können im Logik-Editor verwendet werden.

   Wenn Sie nicht alle Eingangs- oder Ausgangspunkte freigeben möchten, können Sie auch einige bestimmte eingeben. Sie können auch verteilte E/A-Eingänge oder -Ausgänge freigeben, indem Sie an dieser Stelle die entsprechenden Tag-Namen eingeben.

8. Geben Sie einen Namen für das Tag ein, und wählen Sie den Typ aus: BOOL, BYTE, WORD oder DWORD.

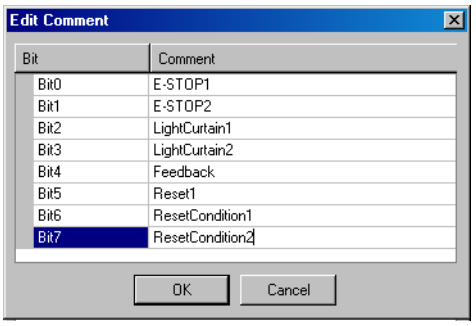


9. Klicken Sie auf „OK“.

10. Gehen Sie zum Erstellen eines Tag-Namens für jedes Bit in einer E/A-Baugruppe wie folgt vor.

a. Wählen Sie die betreffende Baugruppe aus, und klicken Sie auf „Edit Comment“ (Kommentar bearbeiten).

b. Geben Sie für jedes Bit im Tag einen Kommentar ein.



Die hier eingegebenen Tag-Namen-Kommentare werden im Logik-Editor angezeigt.

c. Klicken Sie auf „OK“.

11. Klicken Sie nochmals auf „OK“, um zur Registerkarte „Safety Slave I/O“ (Sicherheits-Slave-E/A) zurückzukehren.

12. Erstellen Sie nach Bedarf zusätzliche Sicherheitseingangs- oder Sicherheitsausgangsbaugruppen für Ihre Anwendung, indem Sie die Schritte 3 bis 11 wiederholen.

13. Wählen Sie zum Speichern Ihrer Konfiguration im Menü „File“ (Datei) die Option „Save“ (Speichern) aus.

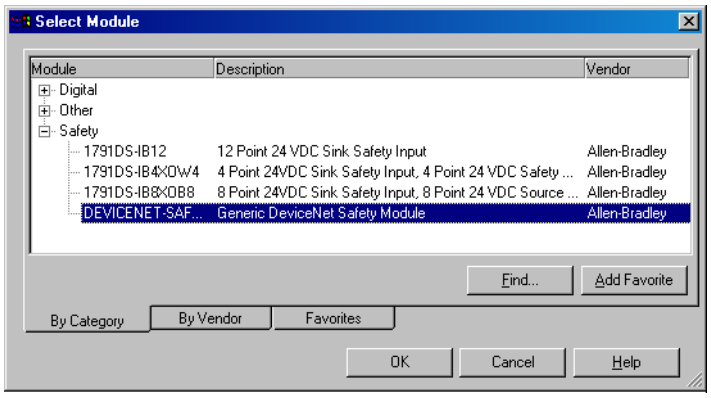
Arbeiten mit dem generischen Sicherheitsprofil in RSLogix 5000

Die Verbindung mit der SmartGuard-Slave-Steuerung können Sie über das generische Sicherheitsprofil in RSLogix 5000 herstellen.

Gehen Sie folgendermaßen vor, um die Verbindung mit der Steuerung herzustellen.

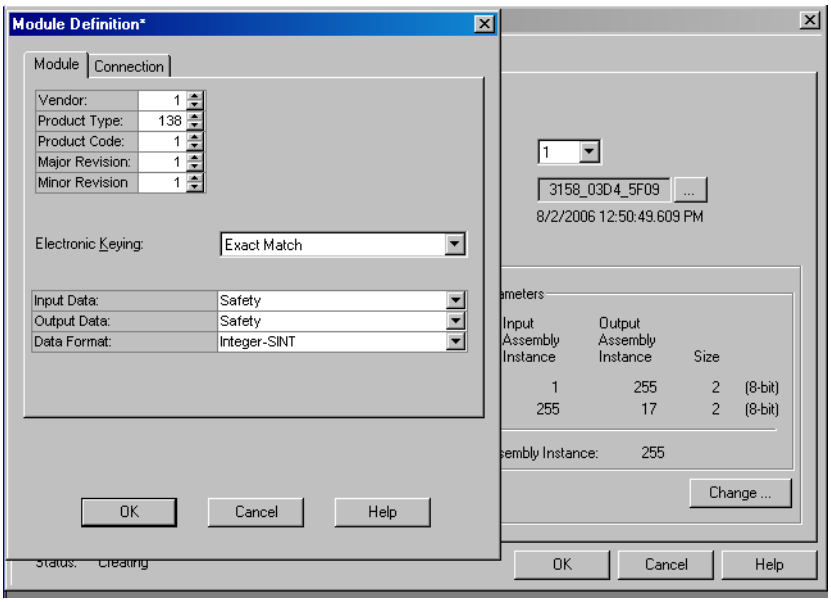
1. Klicken Sie in RSLogix 5000 mit der rechten Maustaste auf das DeviceNet-Netzwerk, und wählen Sie „New Module“ (Neues Modul) aus.

2. Wählen Sie „Generic DeviceNet Safety Module“ (Generisches DeviceNet Safety-Modul) aus, und klicken Sie auf „OK“.

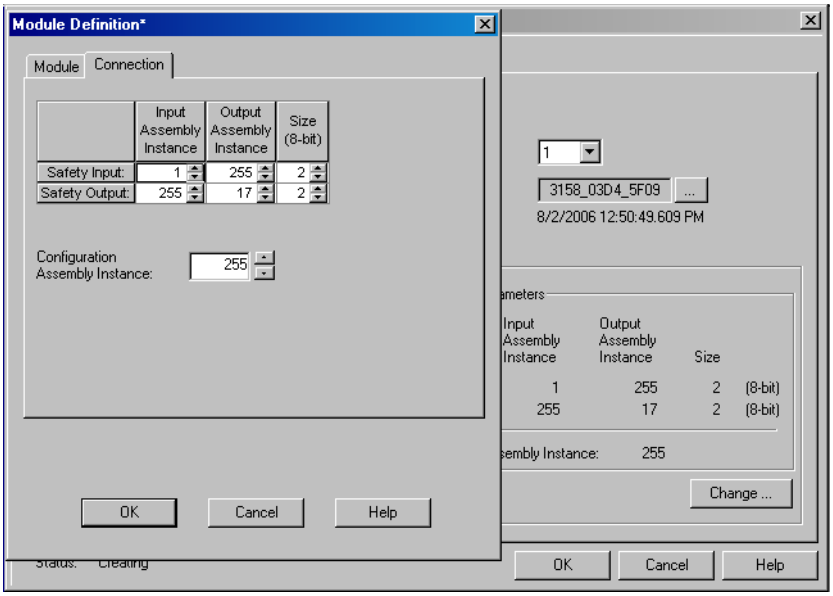


3. Klicken Sie im Dialogfeld „New Module“ (Neues Modul) auf „Change“ (Ändern).

4. Stellen Sie im Dialogfeld „Module Definition“ (Moduldefinition) die Parameter wie dargestellt ein.



5. Klicken Sie auf der Registerkarte „Module Definition“ (Moduldefinition) auf die Registerkarte „Connection“ (Verbindung).



6. Stellen Sie die Sicherheitseingangs- und Sicherheitsausgangsparameter anhand der folgenden Tabellen ein.

Eingangsbaugruppen

Name des Sicherheits-Slave-Eingangs	Eingangsinstanznummer im generischen Profil	Ausgangsinstanznummer im generischen Profil
Sicherheitseingang 1	1	255
Sicherheitseingang 2	2	255
Sicherheitseingang 3	3	255
Sicherheitseingang 4	4	255

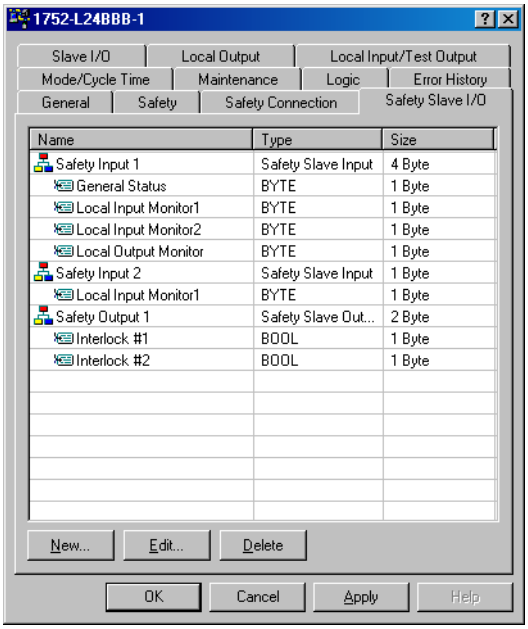
Ausgangsbaugruppen

Name des Sicherheits-Slave-Ausgangs	Eingangsinstanznummer im generischen Profil	Ausgangsinstanznummer im generischen Profil
Sicherheitsausgang 1	255	17 (für 0x11)
Sicherheitsausgang 2	255	18 (für 0x12)
Sicherheitsausgang 3	255	19 (für 0x13)
Sicherheitsausgang 4	255	20 (für 0x14)

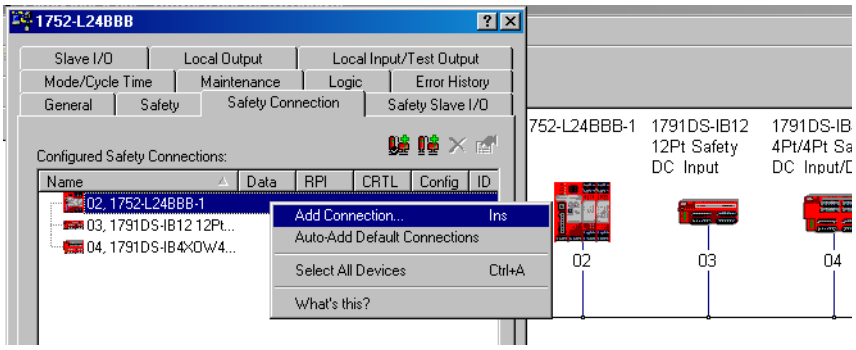
Verriegelungslogik zwischen zwei SmartGuard-Steuerungen

Mittels einer Verriegelungslogik können zwei SmartGuard-Steuerungen dieselben Sicherheitsdaten verwenden und Entscheidungen anhand der Eingänge oder Ausgänge der jeweils anderen Steuerung treffen. Die Verriegelungslogik ermöglicht es, die Sicherheitssteuerung auf mehrere, aufeinander abgestimmte SmartGuard-Steuerungen zu verteilen.

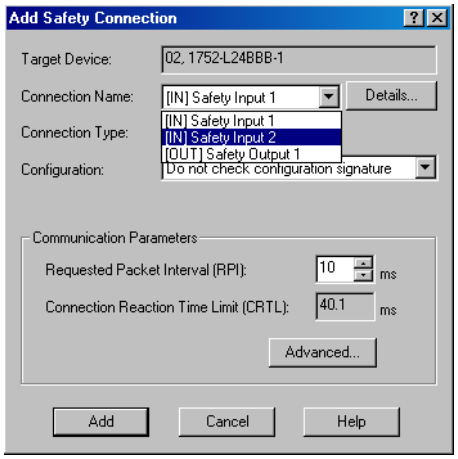
1. Konfigurieren Sie die Sicherheits-Slave-E/A für eine der SmartGuard-Steuerungen wie im Abschnitt Erstellen von Sicherheits-Slave-E/A-Daten auf Seite 90 beschrieben.



2. Auf der Registerkarte „Safety Connections“ (Sicherheitsverbindungen) der anderen SmartGuard-Steuerung wird diese als Sicherheits-Master angegeben. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung und wählen Sie „Add Connection“ (Verbindung hinzufügen) aus.

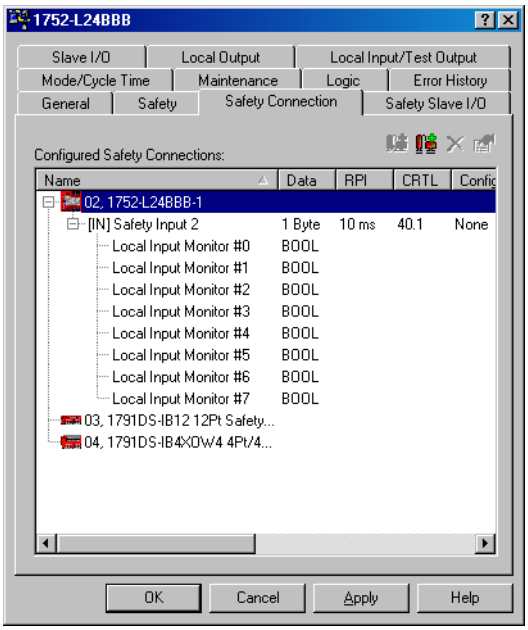


3. Wählen Sie im Dropdown-Menü „Connection Name“ (Verbindungsname) die gewünschte Sicherheits-E/A-Baugruppe aus.



4. Klicken Sie auf „Add“ (Hinzufügen).

   Nun kann die als Sicherheits-Master eingesetzte SmartGuard-Steuerung die Eingänge der anderen SmartGuard-Steuerung, 0 bis 7, lesen.



Konfigurieren der Steuerung als DeviceNet-Standard-Slave

Als DeviceNet-Standard-Slave kann die Steuerung Standard-E/A-Kommunikationsvorgänge mit 1 Standard-Master für bis zu 2 Verbindungen durchführen, indem sie bis zu 16 Byte pro Verbindung verwendet (128 Byte für die Eingangsdaten bei der EtherNet/IP-Kommunikation). Die SmartGuard-Steuerung kann auch auf explizite Standardmeldungen reagieren.

Im Standard-Master können die internen Statusinformationen der Steuerung und ein angegebener E/A-Bereich zugeordnet werden.

WICHTIG Daten, die über die Standard-Slave-Verbindung an die SmartGuard-Steuerung geschrieben werden, müssen als Standarddaten behandelt werden und dürfen nicht zum Steuern der Sicherheitsfunktionen im SmartGuard-Anwendungsprogramm verwendet werden.

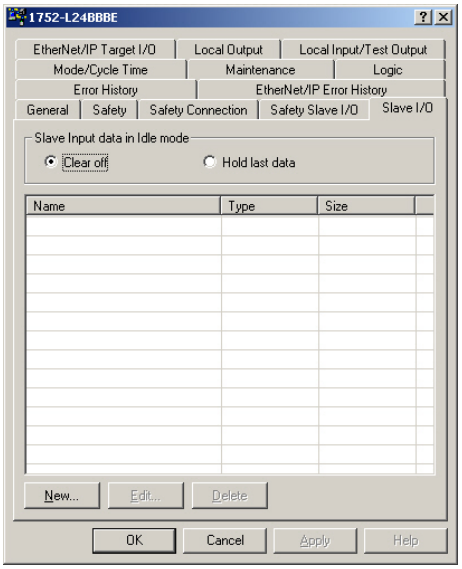
Wenn die SmartGuard-Steuerung Standard-E/A-Kommunikationsvorgänge als Standard-Slave ausführen soll, müssen Standard-Slave-E/A-Daten erstellt und auf dem Standard-Master E/A-Verbindungen konfiguriert werden.

Erstellen von Standard-Slave-E/A-Daten

Gehen Sie folgendermaßen vor, um Standard-Slave-E/A-Baugruppen zu erstellen.

1. Klicken Sie in RSNetWorx for DeviceNet mit der rechten Maustaste auf die SmartGuard-Steuerung, die als Standard-Slave eingesetzt werden soll, und wählen Sie dann „Properties“ (Eigenschaften) aus.

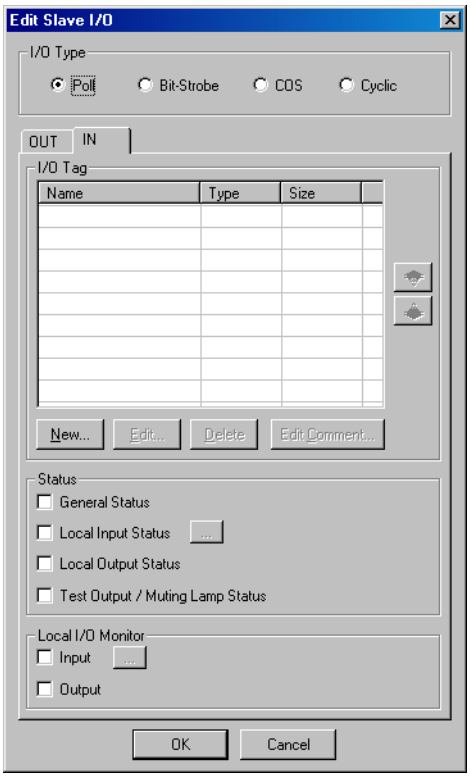
2. Klicken Sie auf die Registerkarte „Slave I/O“ (Slave-E/A).



3. Konfigurieren Sie die Slave-Steuerung für folgende Fälle so, dass die letzten Daten, die von der Slave-Steuerung für eine Eingangsbaugruppe an den Standard-Master gesendet wurden, gelöscht oder gespeichert werden:
   - die Slave-Steuerung wechselt vom Run- in den Idle-Modus.
   - die Steuerung erkennt einen Fehler, etwa einen Kommunikationsfehler in einer Sicherheitskette, welche die Daten an ein E/A-Tag in einer Eingangsbaugruppe festlegt.

4. Klicken Sie auf „New“ (Neu).

5. Klicken Sie auf den E/A-Typ: Abfrage, Bit-Strobe, Zustandswechsel oder Zyklisch.



Die Ausgangsdaten können keine Bit-Strobe-Verbindungen verwenden, da Bit-Strobe-Daten vom Standard-Master nicht ausgegeben werden können. Zudem beträgt die maximale Größe von Bit-Strobe-Eingangsdaten für den Standard-Master 8 Byte. Zustandswechsel-bedingte und zyklische Verbindungen können nicht gleichzeitig verwendet werden.

6. Aktivieren Sie zum Hinzufügen von Statusinformationen für Eingangstypen das entsprechende Kontrollkästchen im Bereich „Status“ (optional).

   Wenn der E/A-Typ Eingang ist, können Sie die folgenden Statusinformationen in die E/A-Baugruppe einbeziehen.

Tag-Name	Datengröße	Attributtyp
Allgemeiner Status	Byte	Standard
Status zentraler Eingang	Wort	Standard
Status zentraler Ausgang	Byte	Standard
Status Testausgang/Muting-Lampe	Byte	Standard

7. Zum Hinzufügen zentraler E/A-Überwachungsdaten für Eingangstypen überprüfen Sie das entsprechende Kontrollkästchen im Bereich „Local I/O Monitor“ (Zentrale E/A-Überwachung).

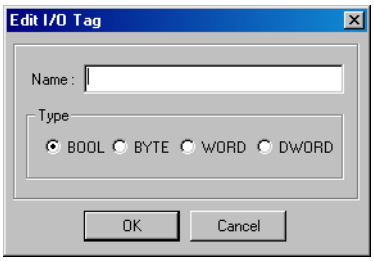
Tag-Name	Datengröße	Attributtyp
Überwachung zentraler Eingang 1 (Eingänge 0 bis 7)	Byte	Standard
Überwachung zentraler Eingang 2 (Eingänge 8 bis 15)	Byte	Standard
Überwachung zentraler Ausgang (Ausgänge 0 bis 7)	Byte	Standard

   Ausgangstypen dürfen keine zentralen E/A-Überwachungsdaten enthalten. Eingangs- und Ausgangswerte können nur gelesen und nicht direkt geschrieben werden.

8. Klicken Sie auf „New“ (Neu), um ein E/A-Tag zu erstellen.

   In einer E/A-Baugruppe können mehrere E/A-Tags definiert werden. In jeder E/A-Baugruppe können E/A-Tags für bis zu 16 Bytes definiert werden. Die dort definierten E/A-Tags können im Logik-Editor verwendet werden.

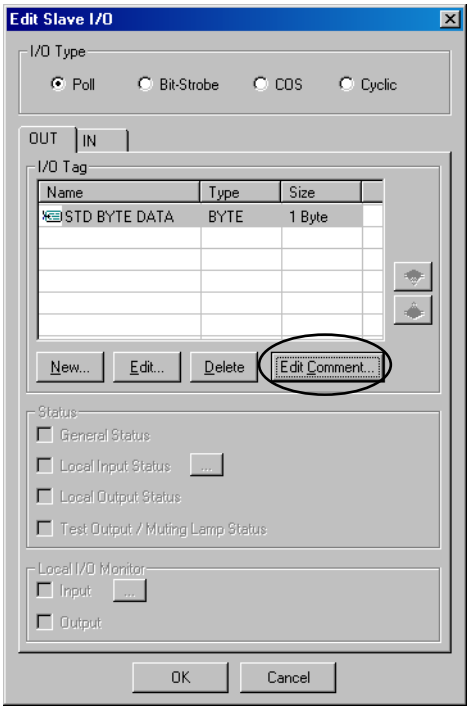
9. Geben Sie einen Namen für das Tag ein und klicken Sie auf den Typ: BOOL, BYTE, WORD oder DWORD.



10. Klicken Sie auf „OK“.

11. Gehen Sie zum Erstellen eines Tag-Namens für jedes Bit in einer E/A-Baugruppe wie folgt vor.

a. Wählen Sie die betreffende Baugruppe aus, und klicken Sie auf „Edit Comment“ (Kommentar bearbeiten).



b. Geben Sie für jedes Bit im Tag einen Kommentar ein.

Die hier eingegebenen Tag-Namen-Kommentare werden im Logik-Editor angezeigt.

c. Klicken Sie auf „OK“.

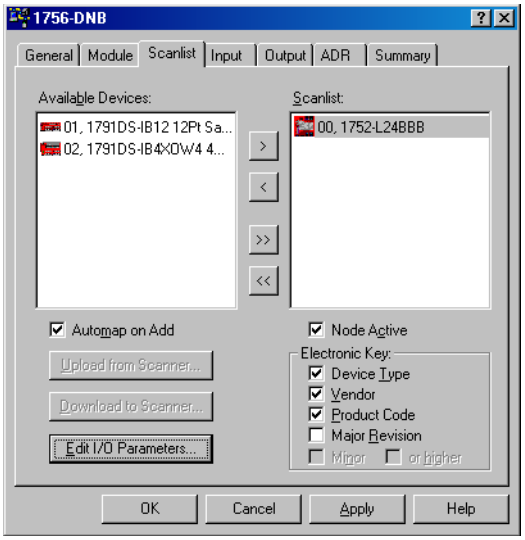
12. Klicken Sie nochmals auf „OK“, um zur Registerkarte „Slave I/O“ (Slave-E/A) zurückzukehren.

13. Erstellen Sie nach Bedarf zusätzliche Eingangs- oder Ausgangsbaugruppen für Ihre Anwendung, indem Sie die Schritte 4 bis 12 wiederholen.

14. Wählen Sie im Menü „File“ (Datei) die Option „Save“ (Speichern) aus, um Ihre Konfiguration zu speichern.

Hinzufügen des SmartGuard-Standard-Slaves zur Abtastliste des Standard-Masters

Um die Standard-Slave-E/A-Baugruppen für den Standard-Master verfügbar zu machen, fügen Sie die SmartGuard-Standard-Slave-Steuerung der Abtastliste des Masters hinzu.



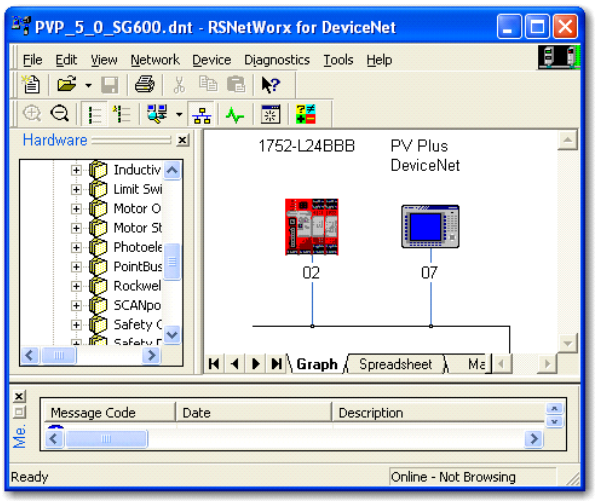
In der Anwenderdokumentation für den Standard-Master finden Sie Informationen zur Konfiguration des betreffenden Geräts.

Speichern Sie die Konfiguration in RSNetWorx for DeviceNet, indem Sie „File > Save“ (Datei > Speichern) auswählen.

Lesen und Schreiben von der und auf die SmartGuard-Steuerung zu einer PanelView Plus-Schnittstelle

In diesem Abschnitt wird beschrieben, wie Sie Daten von der SmartGuard-Steuerung und der PanelView Plus-Schnittstelle lesen und auf diese schreiben. Die SmartGuard-Steuerung ist ein Standard-Slave innerhalb dieser Architektur. Weitere Informationen finden Sie auf Seite 98.

SmartGuard-Steuerung und PanelView Plus-Schnittstelle im Netzwerk

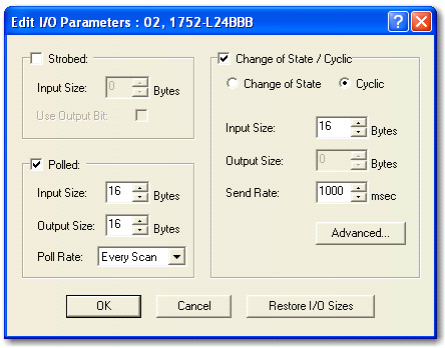


Sie können aus den vier Verbindungstypen bis zu zwei Verbindungen auswählen, doch es kann jeweils nur eine Verbindung jedes Typs hergestellt werden. Beispielsweise kann eine abgefragte Verbindung und eine COS-Verbindung hergestellt werden. Das Herstellen von zwei abgefragten Verbindungen ist dagegen nicht möglich. Abgefragte und COS-/zyklische Verbindungen lassen Ein- und Ausgänge (Lesen und Schreiben) in einer einzigen Verbindung zu.

Eine abgefragte Verbindung, die Ein- und Ausgänge verwendet, kann 16 Byte Eingangsdaten und 16 Byte Ausgangsdaten aufweisen. Wenn Sie eine andere Verbindung hinzufügen, stehen Ihnen 16 zusätzliche Datenbytes zur Verfügung.

Wenn Sie die abgefragte Verbindung verwenden und anschließend eine COS-/zyklische Verbindung hinzufügen, steht der Ausgang nicht zur Verfügung. Im Folgenden ist die maximale Datenkonfiguration dargestellt.

Dialogfeld „Edit I/O Parameters“ (E/A-Parameter bearbeiten)



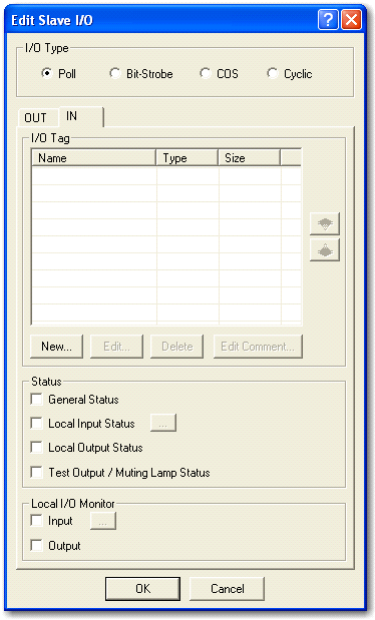
Diese Konfiguration lässt 32 Byte Eingangsdaten (16 über die abgefragte und 16 über die COS- oder zyklische Verbindung) und 16 Byte Ausgangsdaten über die abgefragte Verbindung zu. Diese Konfiguration wird in diesem Kapitel ausführlicher beschrieben.

Lesen von BOOLs aus der SmartGuard-Steuerung und anschließendes Anzeigen der BOOLS auf der PanelView Plus-Schnittstelle

Gehen Sie wie folgt vor, um BOOLs aus der SmartGuard-Steuerung zu lesen und diese auf der PanelView Plus-Schnittstelle anzuzeigen.

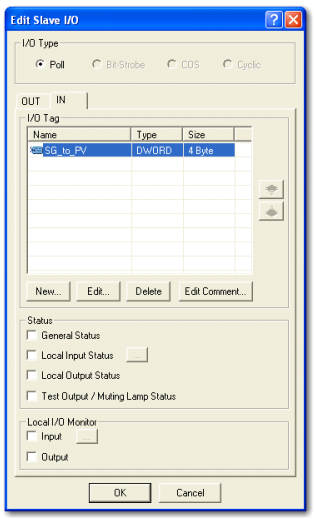
1. Öffnen Sie die Software RSNetWorx.
2. Öffnen Sie die SmartGuard-Eigenschaften.
3. Klicken Sie auf die Registerkarte „Slave I/O“ (Slave-E/A).

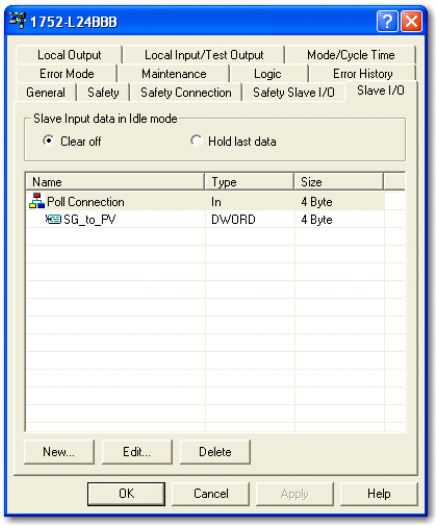
   Das folgende Dialogfeld wird angezeigt.



4. Klicken Sie auf die Registerkarte „IN“ (Eingang).
5. Geben Sie die Tag-Namen ein, die von der PanelView Plus-Schnittstelle gelesen werden.

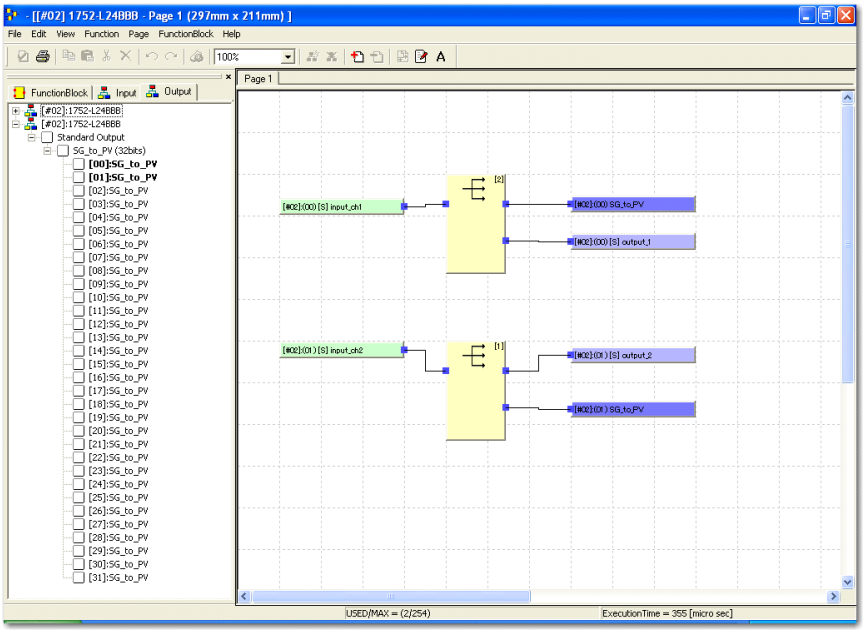
In diesem Fall wurde ein einzelnes 4-Byte-Tag erzeugt und es wird eine abgefragte Verbindung verwendet. Diese 4 Bytes werden von der PanelView Plus-Schnittstelle gelesen.





Selbst wenn Sie ein DWORD-Tag erzeugt haben, können Sie auf alle 32 Bits von DWORD innerhalb des SmartGuard-Editors zugreifen. Der SmartGuard-Beispielcode steuert zwei der 32 Bits.

Die fett dargestellten Tags in der Tag-Liste werden im Code verwendet.



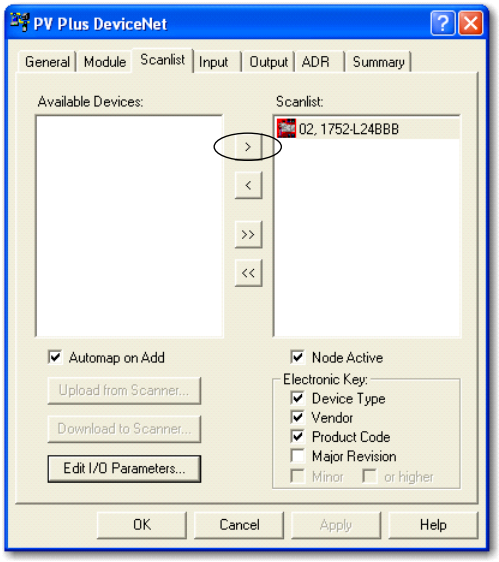
6. Laden Sie die Konfiguration auf die SmartGuard 600-Steuerung herunter.

Konfigurieren der Abtastliste des PanelView-Scanners

Gehen Sie wie folgt vor, um die Abtastliste des DeviceNet-Scanners der PanelView Plus-Serie zu konfigurieren.

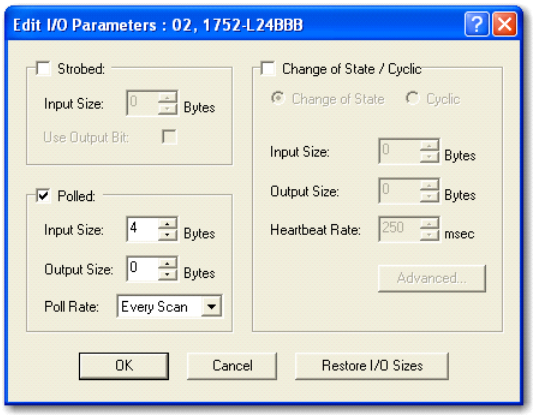
1. Klicken Sie auf die Registerkarte „Scanlist“ (Abtastliste).

2. Klicken Sie auf den Rechtspfeil, um die SmartGuard-Steuerung in die Abtastliste zu verschieben.



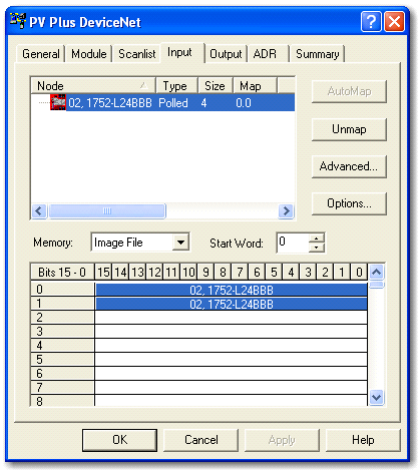
3. Klicken Sie auf „Edit I/O Parameters“ (E/A-Parameter bearbeiten) und stellen Sie sicher, dass das Dialogfeld wie folgt konfiguriert ist.

   Das Beispiel zeigt eine abgefragte 4-Byte-Verbindung, die als Eingang zur PanelView Plus-Schnittstelle dienen soll.



   Da „Automap on Add“ (Automatische Zuordnung beim Hinzufügen) aktiviert war, wurde die folgende Zuordnung automatisch vorgenommen.

4. Stellen Sie sicher, dass die 4 Bytes der Eingangsdaten wie folgt zugeordnet sind.



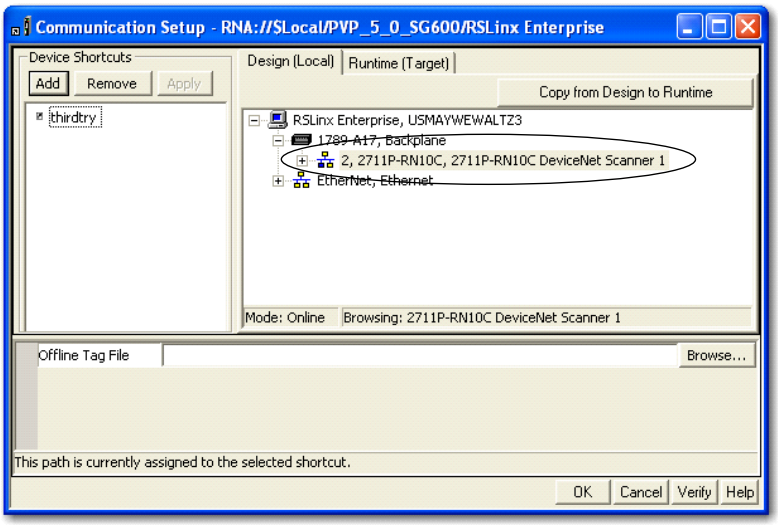
5. Klicken Sie in der Software RSNetWorx mit der rechten Maustaste auf die PanelView Plus-Schnittstelle und wählen Sie „Download to Device“ (Auf Gerät herunterladen) aus.

Konfigurieren Sie den RN10C-DeviceNet-Scanner

Gehen Sie wie folgt vor, um den RN10C-DeviceNet-Scanner zu konfigurieren.

Die Verknüpfung sollte in der Software RSLinx Enterprise ähnlich aussehen wie hier dargestellt.

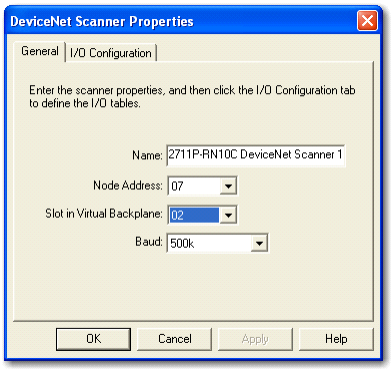
Beachten Sie, dass die Steckplatznummer des RN10C-Scanners 2 lautet.



1. Klicken Sie mit der rechten Maustaste auf den RN10C-Scanner und wählen Sie „Properties“ (Eigenschaften) aus.

2. Geben Sie den Namen des Scanners ein.

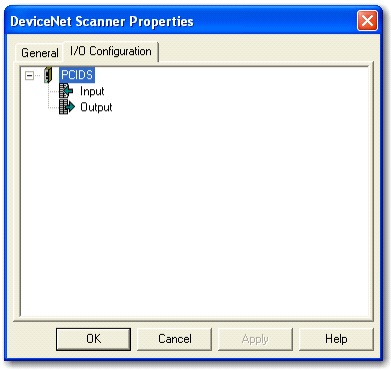
3. Wählen Sie im entsprechenden Pulldown-Menü die Netzknotenadresse, den Steckplatz in der virtuellen Backplane und die Baudrate aus.



Die PanelView Plus-Schnittstelle ist für DeviceNet-Netzknoten 7 konfiguriert. Die DIP-Schalter der SmartGuard-Steuerung sind so eingestellt, dass die automatische Erkennung (links/links/links/rechts von oben nach unten) aktiviert ist. Wählen Sie die richtige Baudrate für Ihre Anwendung aus.

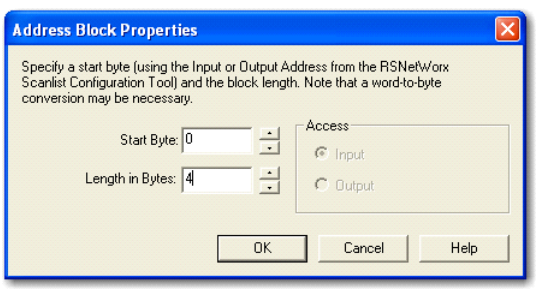
4. Klicken Sie auf die Registerkarte „I/O Configuration“ (E/A-Konfiguration).

Das folgende Dialogfeld wird angezeigt.



5. Klicken Sie mit der rechten Maustaste auf „Input“ (Eingang) und wählen Sie „Add Address Block“ (Adressblock hinzufügen) aus.

Das folgende Dialogfeld wird angezeigt.

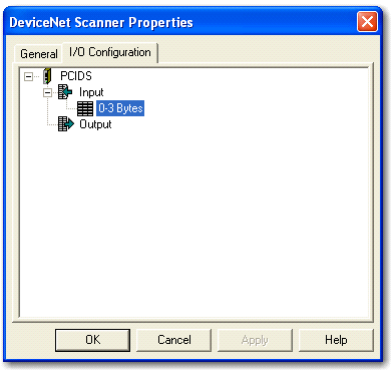


6. Geben Sie in das Feld „Length in Bytes“ (Länge in Byte) den Wert 4 ein.

   Dieser Wert stimmt mit den Daten überein, die der Scanner aus der SmartGuard-Steuerung liest.

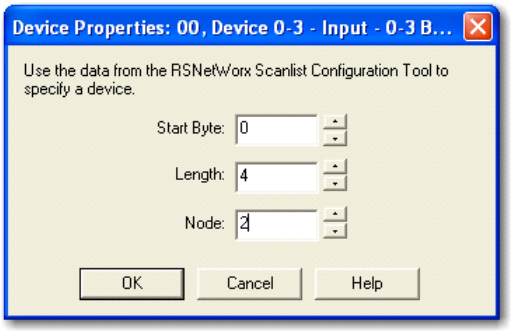
7. Klicken Sie auf „OK“.

   Die E/A-Konfiguration wird angezeigt.



8. Klicken Sie mit der rechten Maustaste auf „0-3 Bytes“ und wählen Sie „Add Devices“ (Geräte hinzufügen) aus.

   Das folgende Dialogfeld wird angezeigt.

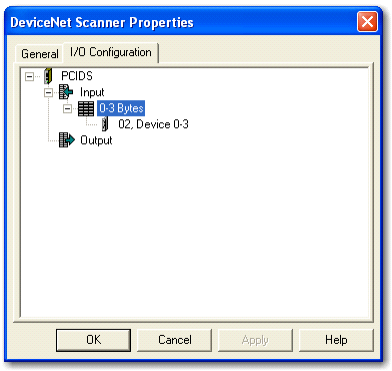


9. Legen Sie die Netzknotennummer so fest, dass sie mit Ihrer SmartGuard-Steuerung übereinstimmt.

   Die Netzknotennummer in diesem Beispiel lautet 2.

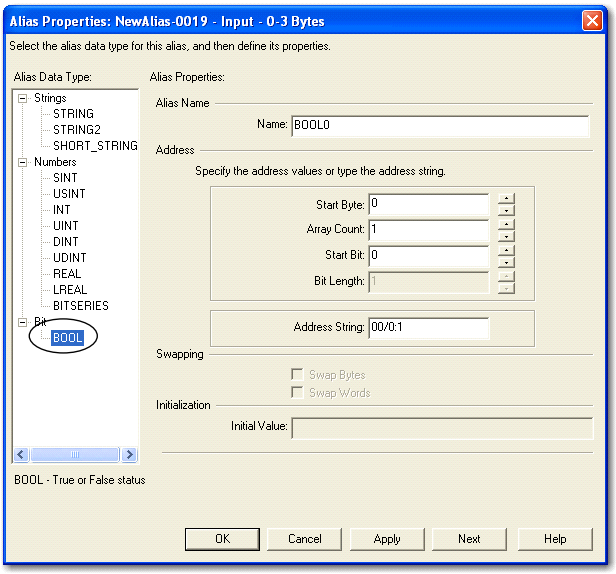
10. Klicken Sie auf „OK“.

    Das folgende Dialogfeld wird angezeigt.



11. Klicken Sie mit der rechten Maustaste auf „0-3 Bytes“ und wählen Sie „Add Alias“ (Aliasnamen hinzufügen) aus.

    Das folgende Dialogfeld wird angezeigt.



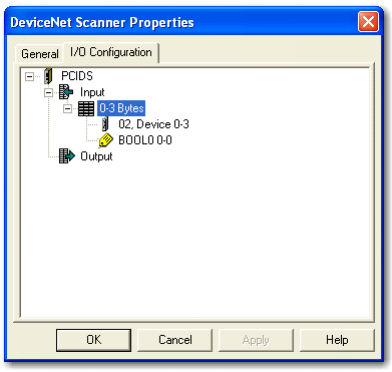
12. Wählen Sie den fett dargestellten Datentyp (BOOL) und aus dem entsprechenden Pulldown-Menü die Optionen „Start Byte“ (Start-Byte), „Array Count“ (Anzahl der Datenfelder) und „Start Bit“ (Start-Bit) aus.

    Die oben dargestellten Werte stehen für Bit 0 des ersten Bytes.

13. Geben Sie den Namen ein.

14. Klicken Sie auf „OK“.

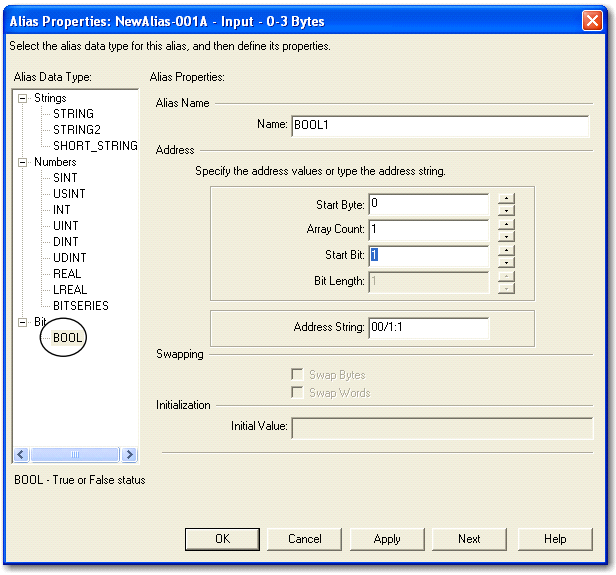
Das folgende Dialogfeld wird angezeigt.



Gehen Sie zum Hinzufügen eines zweiten BOOL-Datentyps, das Bit 1 des ersten Bytes darstellt, wie folgt vor.

1. Klicken Sie mit der rechten Maustaste auf „0-3 Bytes“ und wählen Sie „Add Alias“ (Aliasnamen hinzufügen) aus.

   Wenn der Datentyp BOOL ausgewählt wurde, wird das folgende Dialogfeld angezeigt.

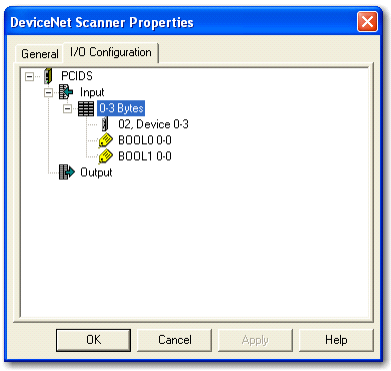


2. Wählen Sie im entsprechenden Pulldown-Menü die Optionen „Start Byte“ (Start-Byte), „Array Count“ (Anzahl der Datenfelder) und „Start Bit“ (Start-Bit) aus.

3. Geben Sie den Namen ein.

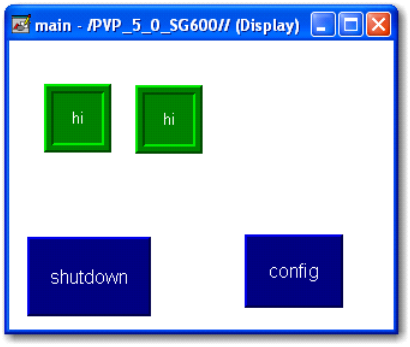
4. Klicken Sie auf „OK“.

   Das folgende Dialogfeld wird angezeigt.

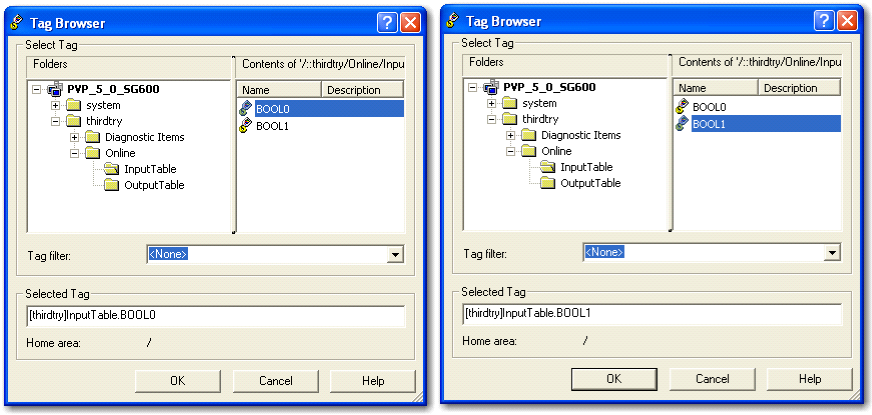


5. Klicken Sie auf „OK“.

Im letzten Schritt wird die PanelView Plus-Grafik erzeugt, die die Alias-Tags anzeigt. In diesem Beispiel werden zwei Anzeigeelemente mit mehreren Zuständen verwendet, die die beiden Aliasnamen anzeigen.



Die Tags für jedes dieser Anzeigeelemente mit mehreren Zuständen können mithilfe der Software RSLinx Enterprise durchsucht werden. Wählen Sie die Tags wie dargestellt aus.



Schließlich müssen Sie Ihr Projekt speichern, eine Laufzeitdatei generieren und diese auf die PanelView Plus-Schnittstelle herunterladen.

Gleichzeitiges Lesen und Schreiben von der und auf die SmartGuard-Steuerung von der PanelView Plus-Schnittstelle aus

Dieses Beispiel zeigt, wie Sie zwei rastende Drucktasten auf einem PanelView Plus-Bildschirm verwenden, um zwei Tags in der SmartGuard 600-Steuerung zu steuern. Hierfür wird ein einzelnes Datenbyte von der PanelView Plus-Schnittstelle zur SmartGuard-Steuerung gesendet. BOOL ist weder in den Eigenschaften des PanelView Plus-Scanners noch auf der SmartGuard-Steuerung vorhanden. Selbst wenn Sie ein BOOL-Tag in der SmartGuard-Steuerung erstellen, um Daten von der PanelView Plus-Schnittstelle zu akzeptieren, wird ein Datenbyte verwendet.

Außerdem existieren in der SmartGuard-Steuerung keine ganzzahligen Werte, auf die Sie über das Programm zugreifen können. Da nur boolesche Datenwerte an die SmartGuard-Steuerung gesendet werden und der kleinste Datentyp in der SmartGuard-Steuerung ein Byte ist, gibt es keinen Grund, weniger als ein Byte von der PanelView Plus-Schnittstelle an die SmartGuard-Steuerung zu senden, selbst wenn Sie nur ein paar Bits verwenden. In diesem Beispiel wird ein Byte Ausgangsdaten konfiguriert, das an die SmartGuard-Steuerung gesendet werden soll. Dabei werden nur zwei Schaltflächen verwendet. Wenn Sie von der PanelView Plus-Schnittstelle aus mehr als acht BOOLs an die SmartGuard-Steuerung senden möchten, bearbeiten Sie das folgende Beispiel und ändern Sie 1 Byte in *x* Bytes in den Ausgangsparametern.

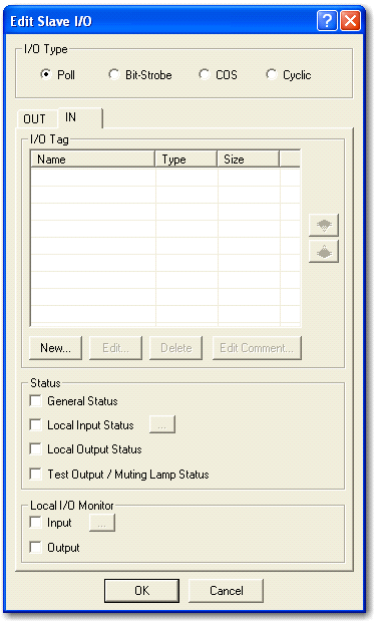
Tags, die von der PanelView Plus-Schnittstelle gelesen werden, müssen auf der Registerkarte „IN“ (Eingang) eingegeben werden.

Tags, die von der PanelView Plus-Schnittstelle geändert werden, müssen auf der Registerkarte „OUT“ (Ausgang) eingegeben werden.

Gehen Sie wie folgt vor, um von der PanelView Plus-Schnittstelle aus gleichzeitig Daten von der und auf die SmartGuard-Steuerung zu lesen und zu schreiben.

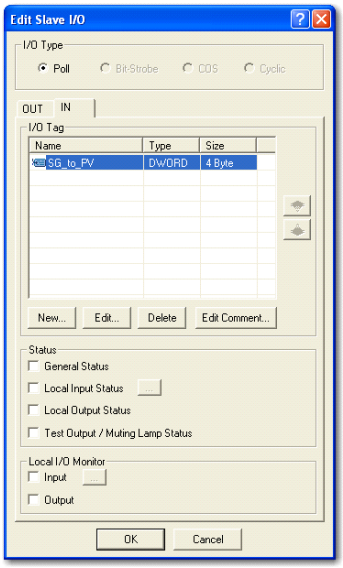
1. Öffnen Sie die Software RSNetWorx.
2. Öffnen Sie die SmartGuard-Eigenschaften.
3. Klicken Sie auf die Registerkarte „Slave I/O“ (Slave-E/A).

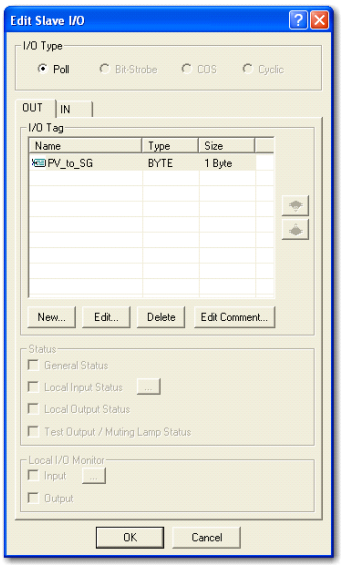
Das folgende Dialogfeld wird angezeigt.

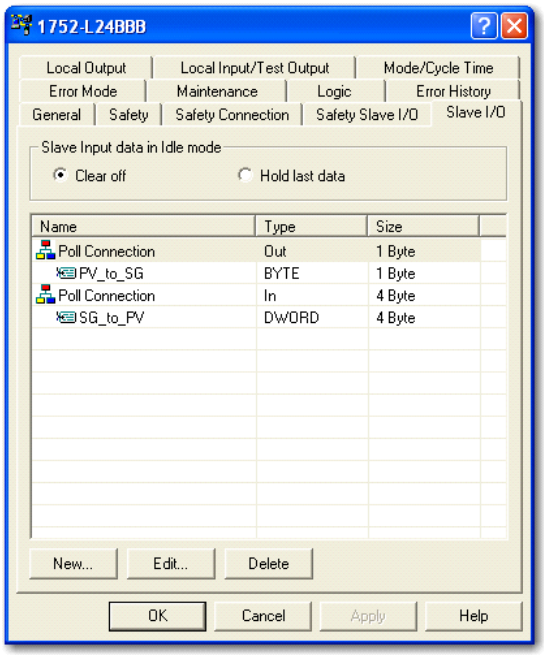


4. Klicken Sie auf die Registerkarte „IN“ (Eingang).
5. Geben Sie die Tag-Namen ein, die von der PanelView Plus-Schnittstelle gelesen werden.
6. Klicken Sie auf die Registerkarte „OUT“ (Ausgang).
7. Geben Sie die Tag-Namen ein, die von der PanelView Plus-Schnittstelle geschrieben werden.

In diesem Fall wird eine abgefragte Verbindung verwendet mit 4 Bytes, die gelesen werden können, und 1 Byte, in das Daten geschrieben werden können.



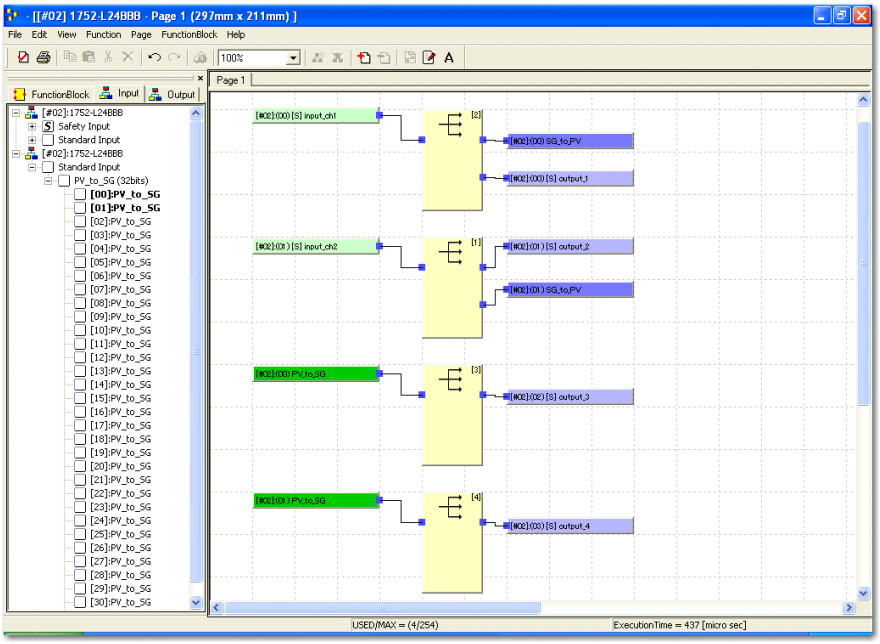




Außerdem haben Sie im SmartGuard-Editor Zugriff auf alle Bits von DWORD und BYTE. Der SmartGuard-Beispielcode verwendet zwei Bits in beiden Puffern.

Die vier fett dargestellten Tags in der Tag-Liste werden im Code verwendet.

Im Folgenden ist die Registerkarte „Input“ (Eingang) abgebildet und es werden die Tags „PV_to_SG“ angezeigt. Klicken Sie zum Einsehen der Tags „SG_to_PV“ auf die Registerkarte „Output“.



8. Laden Sie die Konfiguration auf die SmartGuard 600-Steuerung herunter.

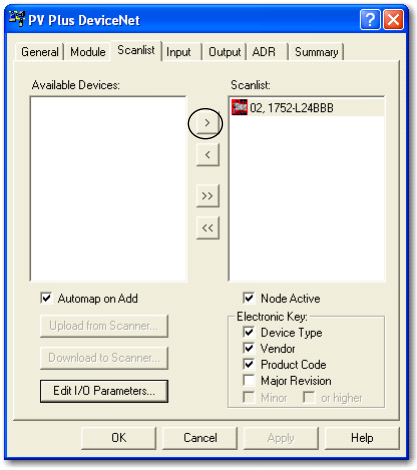
Konfigurieren der Abtastliste des PanelView-Scanners

Sie müssen für den DeviceNet-Scanner der PanelView Plus-Serie die Abtastliste konfigurieren.

Gehen Sie wie folgt vor, um die SmartGuard 600-Steuerung der Abtastliste hinzuzufügen.

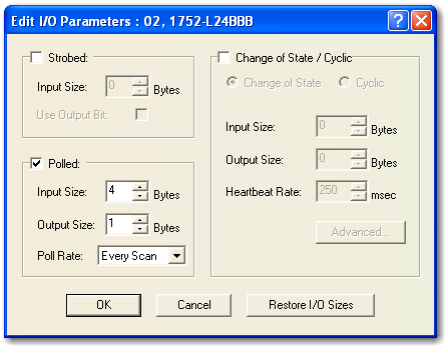
1. Klicken Sie auf die Registerkarte „Scanlist“ (Abtastliste).

2. Klicken Sie auf den Rechtspfeil, um die SmartGuard-Steuerung in die Abtastliste zu verschieben.



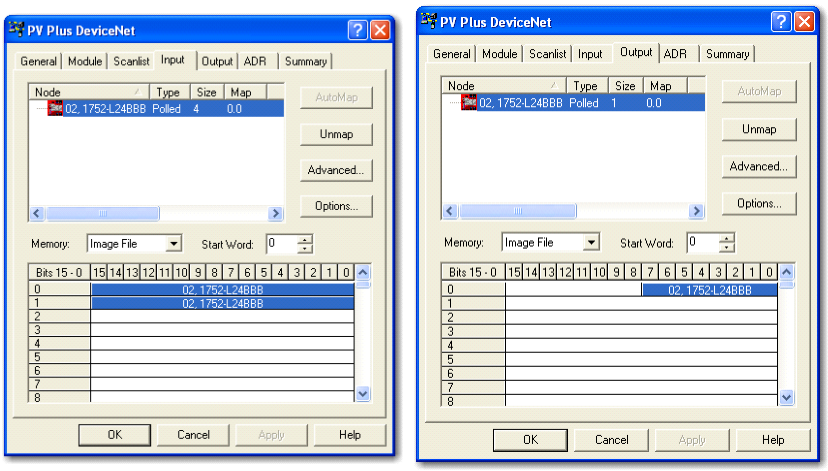
3. Klicken Sie auf „Edit I/O Parameters“ (E/A-Parameter bearbeiten) und stellen Sie sicher, dass das Dialogfeld wie folgt konfiguriert ist.

   Das Beispiel zeigt eine abgefragte Verbindung, die zwischen der SmartGuard-Steuerung und der PanelView Plus-Schnittstelle 4 Bytes liest und 1 Byte schreibt.



   Da „Automap on Add“ (Automatische Zuordnung beim Hinzufügen) aktiviert war, wurde die folgende Zuordnung automatisch vorgenommen.

4. Stellen Sie sicher, dass die 4 Bytes der Eingangsdaten und das eine Byte der Ausgangsdaten wie folgt zugeordnet sind.

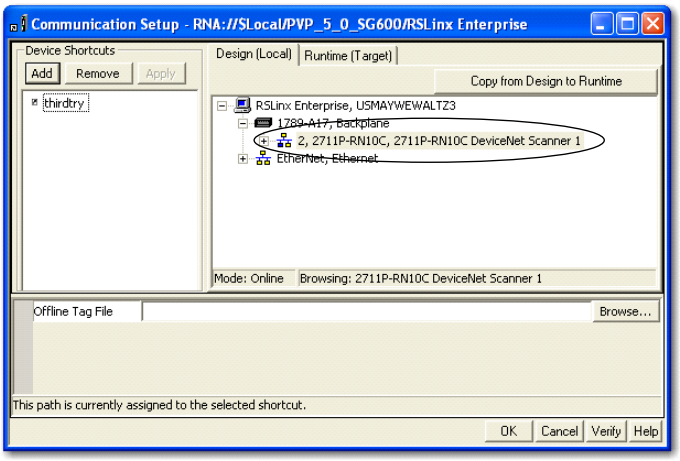


5. Klicken Sie in der Software RSNetWorx mit der rechten Maustaste auf die PanelView Plus-Schnittstelle und wählen Sie „Download to Device“ (Auf Gerät herunterladen) aus, um diese Konfiguration auf die PanelView Plus-Schnittstelle herunterzuladen.

Konfigurieren Sie den RN10C-DeviceNet-Scanner

Gehen Sie wie folgt vor, um den RN10C-DeviceNet-Scanner zu konfigurieren.

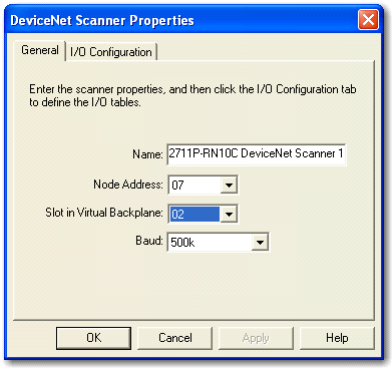
Die Verknüpfung sollte in der Software RSLinx Enterprise ähnlich aussehen wie hier dargestellt.



Beachten Sie, dass die Steckplatznummer des RN10C-Scanners 2 lautet.

1. Klicken Sie mit der rechten Maustaste auf den RN10C-Scanner und wählen Sie „Properties“ (Eigenschaften) aus.

   Das folgende Dialogfeld wird angezeigt.



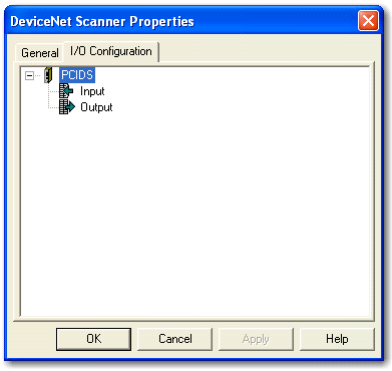
2. Geben Sie den Namen des Scanners ein.

3. Wählen Sie im entsprechenden Pulldown-Menü die Netzknotenadresse, den Steckplatz in der virtuellen Backplane und die Baudrate aus.

   Die PanelView Plus-Schnittstelle ist für DeviceNet-Netzknoten 7 konfiguriert. Die DIP-Schalter der SmartGuard-Steuerung sind so eingestellt, dass die automatische Erkennung (links/links/links/rechts von oben nach unten) aktiviert ist. Wählen Sie die richtige Baudrate für Ihre Anwendung aus.

4. Klicken Sie auf die Registerkarte „I/O Configuration“ (E/A-Konfiguration).

Das folgende Dialogfeld wird angezeigt.



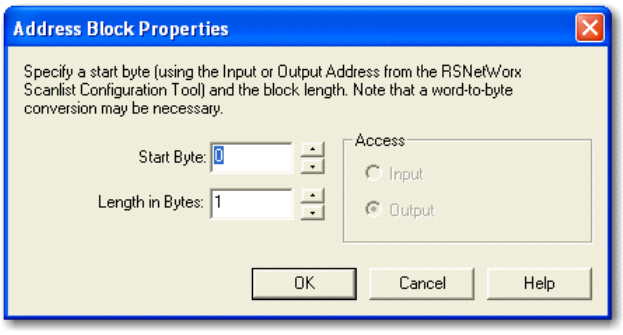
Die Konfiguration des Eingangsblocks wird im Abschnitt zum Lesen von BOOLs in diesem Dokument beschrieben. In diesem Abschnitt finden Sie Informationen zum Konfigurieren der Daten, die von der SmartGuard-Steuerung gelesen und auf der PanelView Plus-Schnittstelle angezeigt werden.

Konfigurieren der Daten, die von der PanelView Plus-Schnittstelle auf die SmartGuard-Steuerung geschrieben werden

Gehen Sie wie folgt vor, um die Daten zu konfigurieren, die von der PanelView Plus-Schnittstelle auf die SmartGuard-Steuerung geschrieben werden.

1. Klicken Sie mit der rechten Maustaste auf „Output“ (Ausgang) und wählen Sie „Add Address Book“ (Adressbuch hinzufügen) aus.

   Das folgende Dialogfeld wird angezeigt.

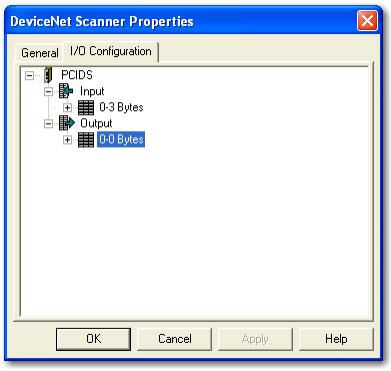


2. Wählen Sie im Feld „Length in Bytes“ (Länge in Byte) den Wert 1 aus.

   Dies stimmt mit den Daten überein, die der Scanner auf die SmartGuard-Steuerung schreibt.

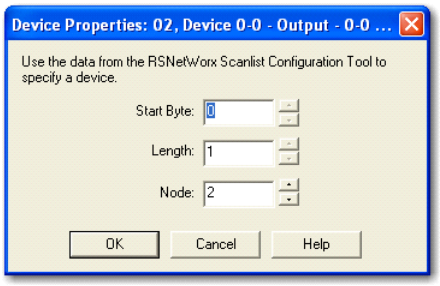
3. Klicken Sie auf „OK“.

Das folgende Dialogfeld wird angezeigt.



4. Klicken Sie mit der rechten Maustaste auf „0-0 Bytes“ und wählen Sie „Add Devices“ (Geräte hinzufügen) aus.

   Das folgende Dialogfeld wird angezeigt.

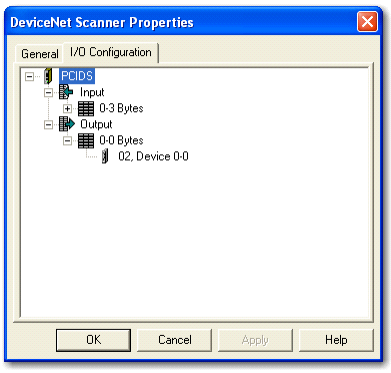


5. Legen Sie die Netzknotennummer so fest, dass sie mit Ihrer SmartGuard-Steuerung übereinstimmt.

   Die Netzknotennummer in diesem Beispiel lautet 2.

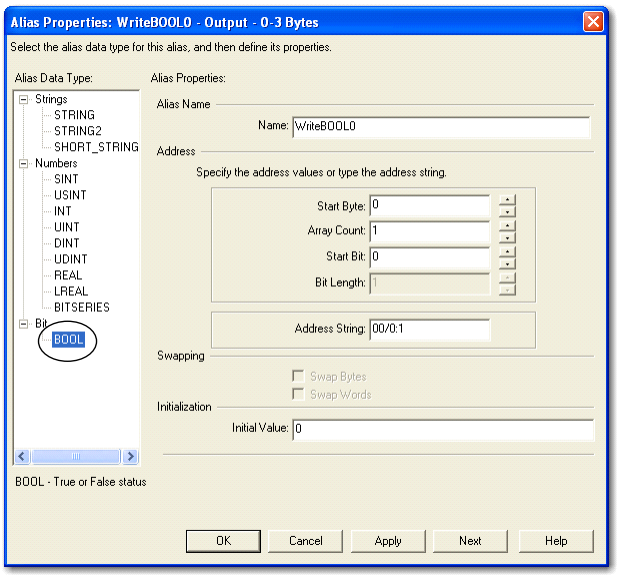
6. Klicken Sie auf „OK“.

   Das folgende Dialogfeld wird angezeigt.



7. Klicken Sie mit der rechten Maustaste auf „0-0 Bytes“ und wählen Sie „Add Alias“ (Aliasnamen hinzufügen) aus.

Wenn der Datentyp BOOL ausgewählt wurde, wird das folgende Dialogfeld angezeigt.



Die oben dargestellten Werte stehen für Bit 0 des ersten Bytes.

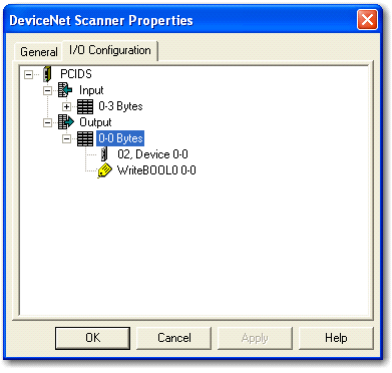
8. Wählen Sie im entsprechenden Pulldown-Menü die Optionen „Start Byte“ (Start-Byte), „Array Count“ (Anzahl der Datenfelder) und „Start Bit“ (Start-Bit) aus.

9. Geben Sie den Namen ein.

10. Geben Sie den Anfangswert 0 ein.

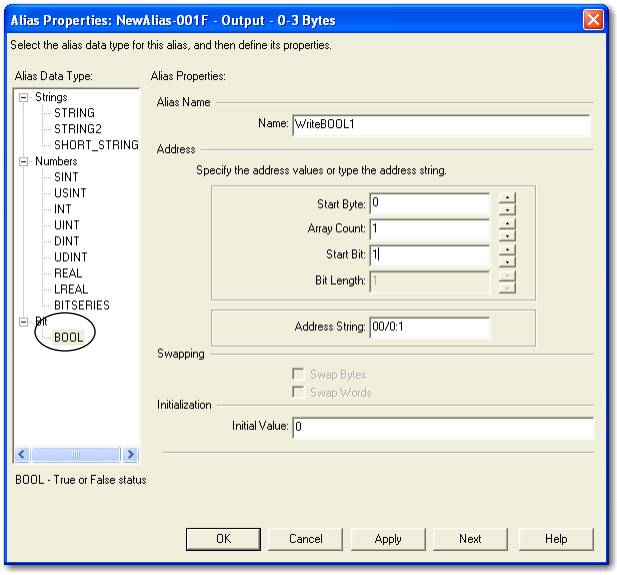
11. Klicken Sie auf „OK“.

    Das folgende Dialogfeld wird angezeigt.



Gehen Sie zum Hinzufügen eines zweiten BOOL-Datentyps, das Bit 1 des ersten Bytes darstellt, wie folgt vor.

1. Klicken Sie mit der rechten Maustaste auf „0-0 Bytes“ und wählen Sie „Add Alias“ (Aliasnamen hinzufügen) aus.



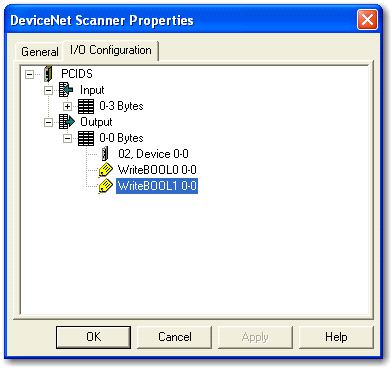
2. Wählen Sie den Datentyp (BOOL) und aus dem entsprechenden Pulldown-Menü die Optionen „Start Byte“ (Start-Byte), „Array Count“ (Anzahl der Datenfelder) und „Start Bit“ (Start-Bit) aus.

3. Geben Sie den Namen ein.

4. Geben Sie den Anfangswert 0 ein.

5. Klicken Sie auf „OK“.

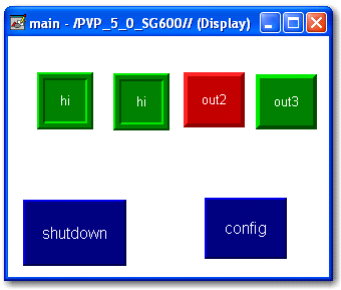
   Das folgende Dialogfeld wird angezeigt.



6. Klicken Sie auf „OK“.

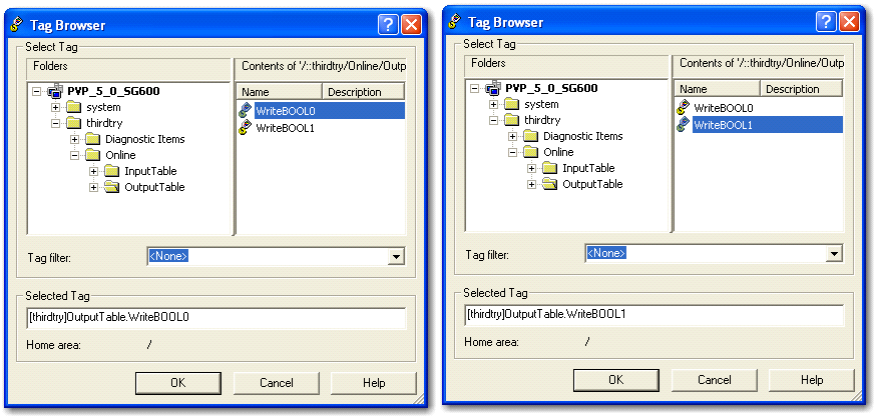
Im letzten Schritt wird die PanelView Plus-Grafik erzeugt, die die Alias-Tags anzeigt. In diesem Beispiel werden zwei rastende Schaltflächen verwendet, die die beiden Aliasnamen anzeigen.

PanelView Plus-Grafik



Die Tags für jede dieser rastenden Schaltflächen können mithilfe der Software RSLinx Enterprise durchsucht werden. Wählen Sie die Tags wie dargestellt aus.

Durchsuchen der Tags für rastende Schaltflächen



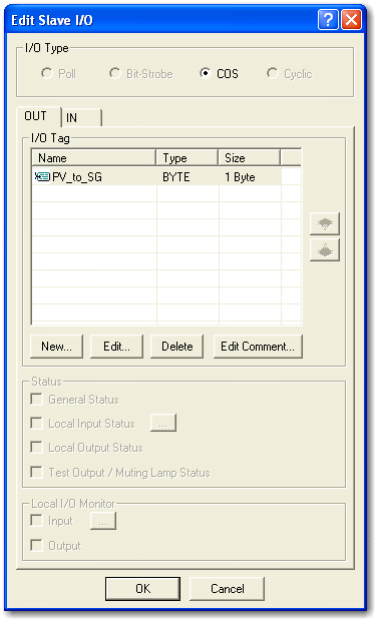
Schließlich müssen Sie Ihr Projekt speichern, eine Laufzeitdatei generieren und diese auf die PanelView Plus-Schnittstelle herunterladen.

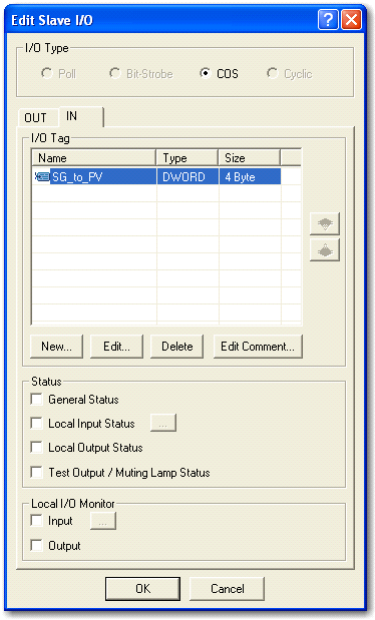
COS vs. abgefragt

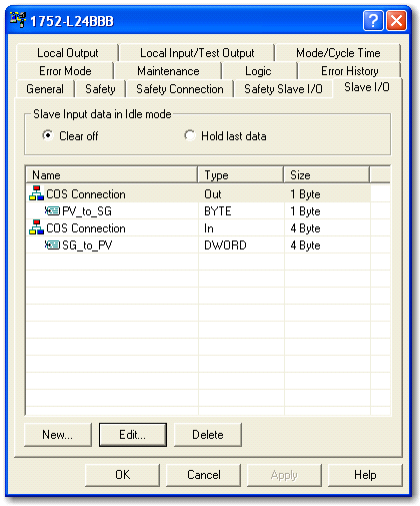
Wenn Sie lieber COS-Verbindungen (Change of State) anstelle von abgefragten Verbindungen verwenden, nehmen Sie die entsprechenden Änderungen von Seite 113 bis zu diesem Abschnitt vor, wie in den folgenden Dialogfeldern veranschaulicht.

Die folgenden Änderungen gelten für die SmartGuard-Slave-E/A-Konfiguration.

Änderungen an der SmartGuard-Slave-E/A-Konfiguration

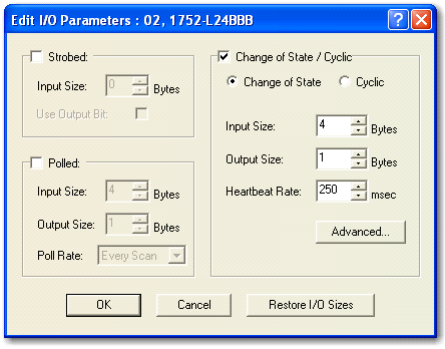


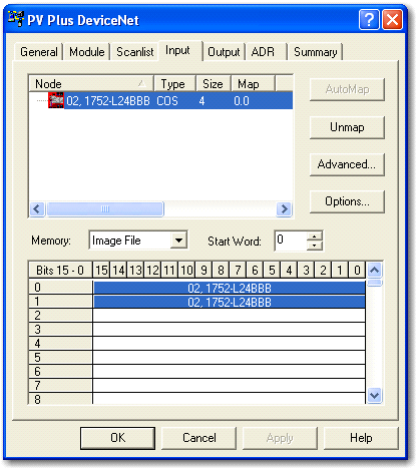


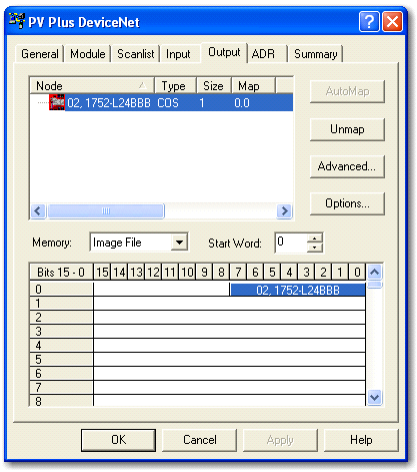


Die folgenden Änderungen gelten für die Konfiguration des RN10C-DeviceNet-Scanners in der Software RSNetWorx.

Änderungen der Konfiguration des RN10C-DeviceNet-Scanners





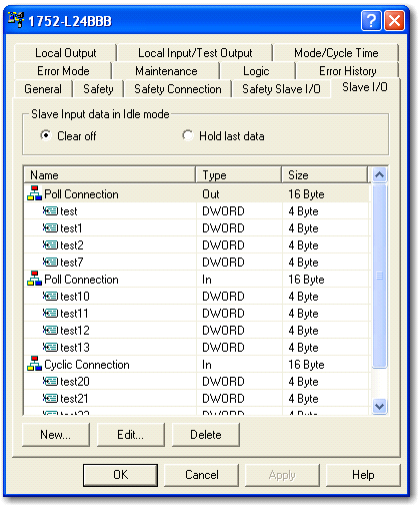


Maximale Verbindungsgrößen

In diesem Beispiel liegt eine abgefragte Verbindung mit 16-Byte-Eingang und 16-Byte-Ausgang vor. Es wurde eine zweite Verbindung (zyklisch) des 16-Byte-Eingangs hinzugefügt. Im Folgenden sehen Sie die Änderungen, die vorgenommen werden müssen, damit die Konfiguration unterstützt wird.

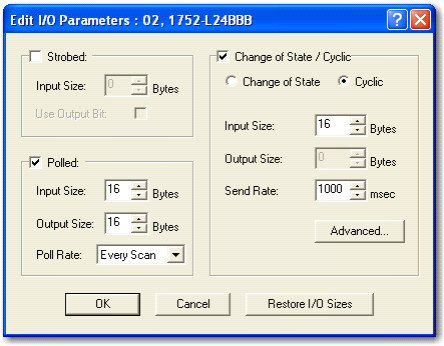
Die SmartGuard-Slave-E/A-Konfiguration wird wie folgt angezeigt.

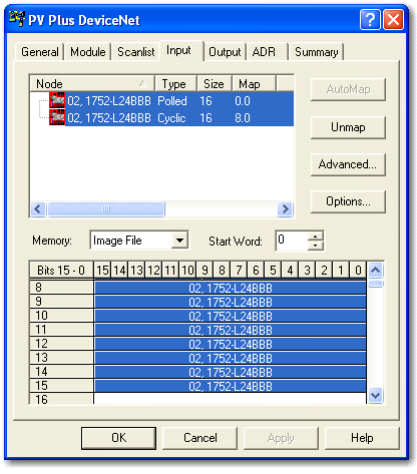
SmartGuard-Slave-E/A-Konfiguration

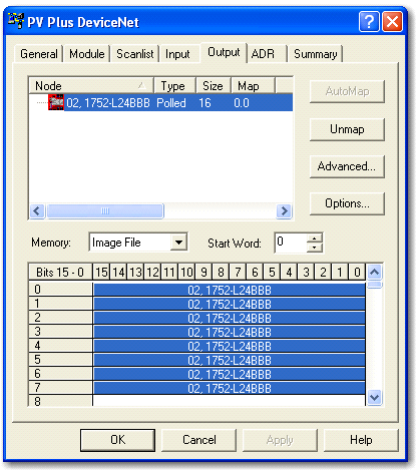


Die Verbindungseigenschaften des DeviceNet-Scanners werden wie folgt angezeigt.

Konfiguration des DeviceNet-Scanners

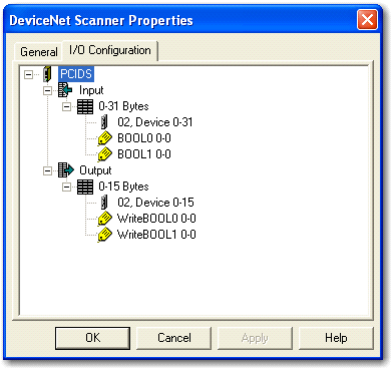






Die E/A-Konfiguration der Software FactoryTalk zur Software RSView Enterprise wird wie folgt dargestellt.

E/A-Konfiguration der Software FactoryTalk zur Software RSView Enterprise



Notizen:

Konfigurieren Ihrer Steuerung für die EtherNet/IP-Kommunikation

Einleitung

Die SmartGuard-Steuerung (Bestellnummer 1752-L24BBBE) bietet EtherNet/IP-Anschlussmöglichkeiten.

Thema	Seite
Konfigurieren der Ziel-E/A in der Software RSNetWorx for DeviceNet	130
Konfigurieren Ihrer Steuerung als Slave mithilfe des generischen Profils der Software RSLogix 5000	134
Konfigurieren der Kommunikation zwischen einem Standard-PanelView-Terminal und einer SmartGuard 600-Steuerung über ein EtherNet/IP-Netzwerk	136

Multicast-Verbindungen

Sie können immer nur zwei Verbindungen zur SmartGuard-Steuerung herstellen. Hierbei kann es sich um einen Eingang und einen Ausgang oder um zwei Eingänge oder zwei Ausgänge handeln. Auch wenn es sich um Multicast-Verbindungen handelt, können nach dem Herstellen der beiden Verbindungen keine weiteren Verbindungen mehr akzeptiert werden.

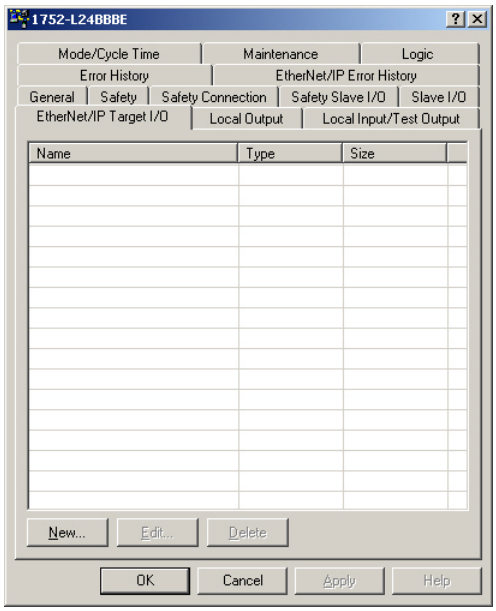
Beispielsweise können Sie mit zwei Steuerungen arbeiten, die an einer Eingangsverbindung der Multicast-Eingangsbaugruppe auf der SmartGuard-Steuerung angeschlossen sind. Hierfür würden die beiden EtherNet/IP-Verbindungen in Anspruch genommen.

Konfigurieren der Ziel-E/A in der Software RSNetWorx for DeviceNet

Gehen Sie wie folgt vor, um Standard-EtherNet/IP-Ziel-E/A-Baugruppen zu erstellen.

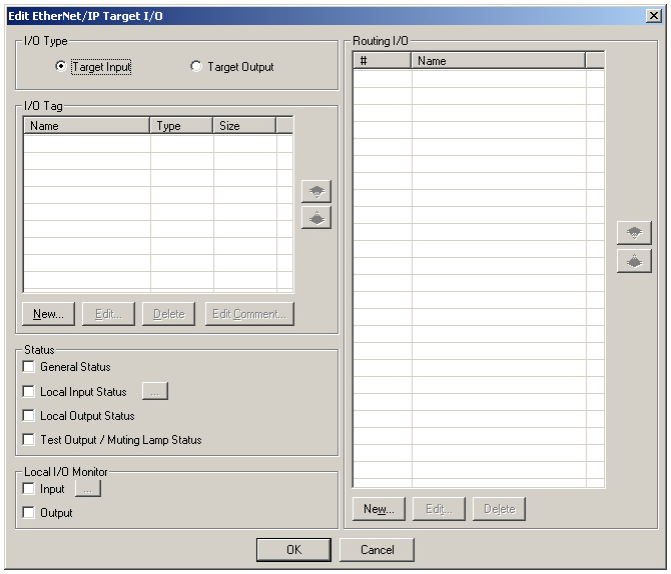
1. Klicken Sie in RSNetWorx for DeviceNet mit der rechten Maustaste auf die SmartGuard-Steuerung und wählen Sie „Properties“ (Eigenschaften) aus.

2. Klicken Sie auf die Registerkarte „EtherNet/IP Target I/O“ (EtherNet/IP-Ziel-E/A).



3. Klicken Sie auf „New“ (Neu).

   Das folgende Dialogfeld wird angezeigt.



4. Klicken Sie im Bereich „I/O Type“ (E/A-Typ) entweder auf „Target Input“ (Zieleingang) oder auf „Target Output“ (Zielausgang).

   Wenn Sie den Zieleingang auswählen, werden diese Daten von der SmartGuard-Steuerung erzeugt und vom Ursprungsgerät gelesen. Wenn Sie den Zielausgang auswählen, werden diese Daten vom Ursprungsgerät erzeugt und an die SmartGuard-Steuerung gesendet.

   Wenn Sie „Target Input“ (Zieleingang) aktiviert haben, können Sie folgende Statusinformationen in die E/A-Baugruppe integrieren.

Tag-Name	Datengröße	Attributtyp
Allgemeiner Status	Byte	Standard
Status zentraler Eingang	Wort	
Status zentraler Ausgang	Byte	
Status Testausgang/Muting-Lampe		

5. Fügen Sie Statusinformationen für Eingangstypen hinzu, indem Sie das entsprechende Kontrollkästchen im Bereich „Status“ aktivieren.

6. Fügen Sie zentrale E/A-Überwachungsdaten für Eingangstypen hinzu, indem Sie das entsprechende Kontrollkästchen für die zentrale E/A-Überwachung aktivieren.

Tag-Name	Datengröße	Attributtyp
Überwachung zentraler Eingang 1 (Eingang 0 bis 7)	Byte	Standard
Überwachung zentraler Eingang 2 (Eingang 8 bis 15)		
Überwachung zentraler Ausgang (Ausgang 0 bis 7)		

   Ausgangstypen dürfen keine zentralen E/A-Überwachungsdaten enthalten. Eingangs- und Ausgangswerte können nur gelesen und nicht direkt geschrieben werden.

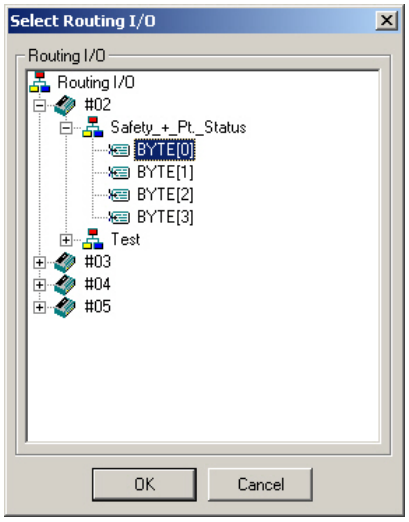
7. Fügen Sie Routing-E/A-Daten für die Module hinzu.

   Wenn die SmartGuard-Steuerung das Sicherheits-DIO-Modul im DeviceNet-Netzwerk steuert, können mithilfe der Funktion „Routing I/O“ (Routing-E/A) die Werte der E/A-Punkte auf den DIO-Modulen an eine Standardsteuerung oder eine HMI-Schnittstelle auf dem EtherNet/IP-Netzwerk weitergeleitet werden.

   TIPP Die Module werden erst dann in der Routing-E/A-Tabelle angezeigt, wenn Sie sie der Sicherheitsabtastliste hinzugefügt und auf „Apply“ (Anwenden) geklickt haben.

   a. Klicken Sie unter „Routing I/O“ (Routing-E/A) auf „New“ (Neu).
   b. Erweitern Sie den Netzknoten, für den Sie Routing-Daten hinzufügen möchten.
   c. Erweitern Sie eine der Baugruppen in der Liste.

d. Wählen Sie das Byte aus, das Sie hinzufügen möchten.



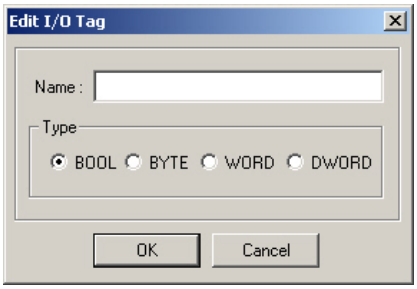
e. Klicken Sie auf „OK“.

f. Wiederholen Sie die Schritte a bis e, um zusätzliche Routing-E/A hinzuzufügen.

8. Klicken Sie unter „I/O Tag“ (E/A-Tag) auf „New“ (Neu), um ein E/A-Tag zu erzeugen.

In einer E/A-Baugruppe können mehrere E/A-Tags definiert werden. In jeder E/A-Baugruppe können E/A-Tags mit bis zu 16 Bytes definiert werden. Die E/A-Tags hier können im Logik-Editor verwendet werden. Beispielsweise können Sie Tags erzeugen, die Fehler aus Befehlen in Ihrem Funktionsblockcode darstellen, und diese anschließend auf einem HMI-Gerät anzeigen.

Das folgende Dialogfeld wird angezeigt.

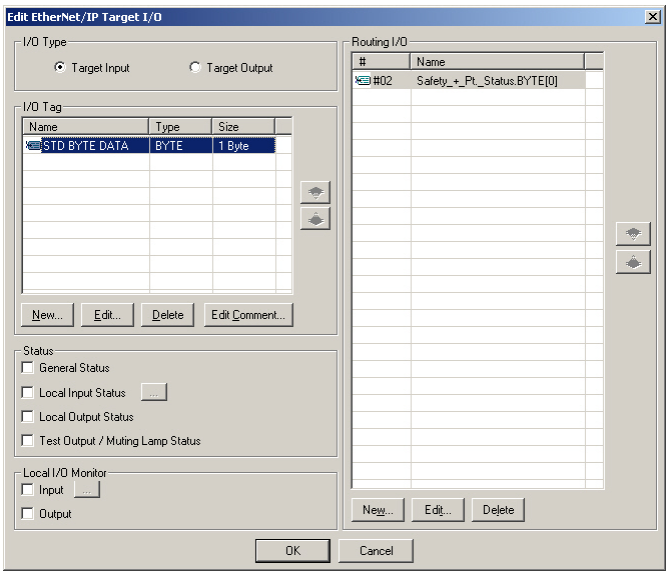


9. Geben Sie einen Namen für das Tag ein und aktivieren Sie den Typ.

Die Optionen lauten BOOL, BYTE, WORD oder DWORD.

10. Klicken Sie auf „OK“.

Das folgende Dialogfeld wird angezeigt.



11. Erstellen Sie einen Tag-Namen für jedes Bit in einer E/A-Baugruppe.

a. Wählen Sie unter „I/O Tag“ (E/A-Tag) die betreffende Baugruppe aus und klicken Sie auf „Edit Comment“ (Kommentar bearbeiten).

b. Geben Sie einen Kommentar für jedes Bit im Tag ein.

Die hier eingegebenen Kommentare zu Tag-Namen werden im Logik-Editor angezeigt.

c. Klicken Sie auf „OK“.

12. Klicken Sie auf „OK“, um zur Registerkarte „EtherNet/IP Target I/O“ (EtherNet/IP-Ziel-E/A) zurückzukehren.

Sie können nach Bedarf zusätzliche Eingangs- oder Ausgangsbaugruppen für Ihre Anwendung erstellen, indem Sie die Schritte 2 bis 11 wiederholen.

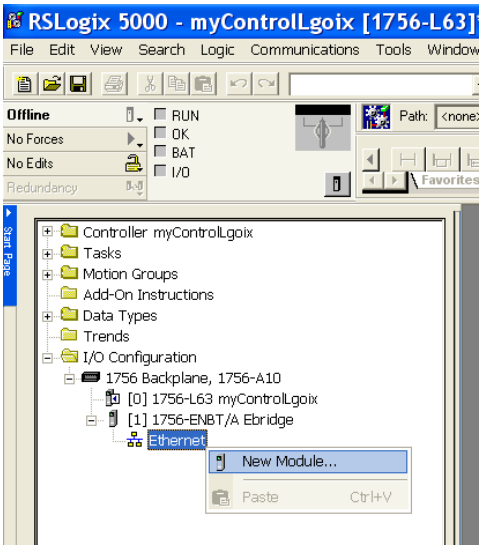
13. Wählen Sie zum Speichern Ihrer Konfiguration im Menü „File“ (Datei) die Option „Save“ (Speichern) aus.

Konfigurieren Ihrer Steuerung als Slave mithilfe des generischen Profils der Software RSLogix 5000

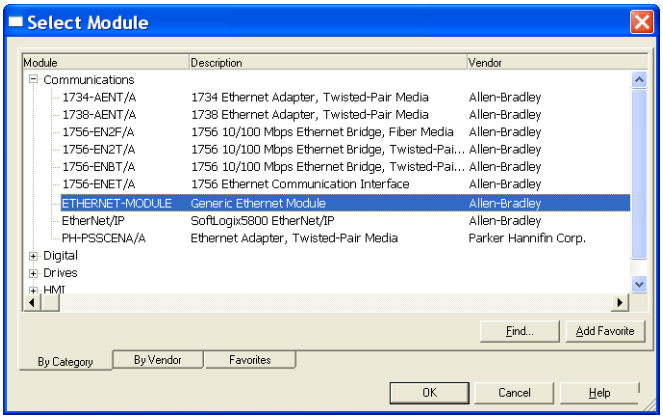
Sobald Sie die gemeinsam zu verwendenden Daten in der SmartGuard-Steuerung konfiguriert haben, können Sie mithilfe der Software RSLogix 5000 und des generischen Standardprofils diese Daten mit einer Logix-Steuerung austauschen.

Gehen Sie folgendermaßen vor, um die Verbindung mit der Steuerung herzustellen.

1. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf das Ethernet-Netzwerk und wählen Sie „New Module“ (Neues Modul) aus.



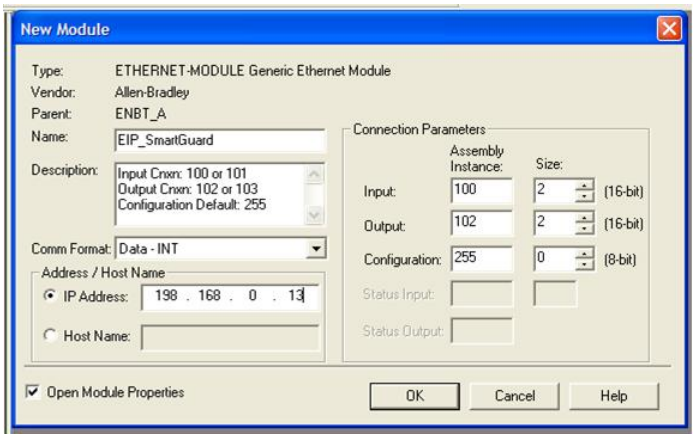
2. Erweitern Sie die Gruppe „Communications“ (Kommunikation) und wählen Sie ETHERNET-MODULE aus.



3. Klicken Sie auf „OK“.

4. Stellen Sie im Dialogfeld „New Module“ (Neues Modul) die Parameter nach Bedarf ein.

In diesem Dialogfeld werden die Instanzwerte für eine Eingang/Ausgang-Verbindung angezeigt.



In der folgenden Tabelle sind die Instanzwerte für eine Eingang/Ausgang-Verbindung und eine reine Eingang-Verbindung aufgeführt.

Verbindungstyp		**Instanznummer**
Eingang/Ausgang	Eingang (SmartGuard-Steuerung zu Steuerung)	100, 101
	Ausgang (Steuerung zu SmartGuard-Steuerung)	102, 103
Nur Eingang	Eingang	100, 101
	Ausgang	199

5. Klicken Sie auf „OK“.

Konfigurieren der Kommunikation zwischen einem Standard-PanelView-Terminal und einer SmartGuard 600-Steuerung über ein EtherNet/IP-Netzwerk

Gehen Sie wie folgt vor, um ein Standard-PanelView-Terminal so zu konfigurieren, dass es mit einer SmartGuard 600-Steuerung über ein EtherNet/IP-Netzwerk kommunizieren kann.

1. Öffnen Sie Ihre PanelView-Anwendung in der Software PanelBuilder32.

   Sie müssen den Kommunikationspfad zwischen dem PanelView-Terminal und der SmartGuard 600-Steuerung definieren.

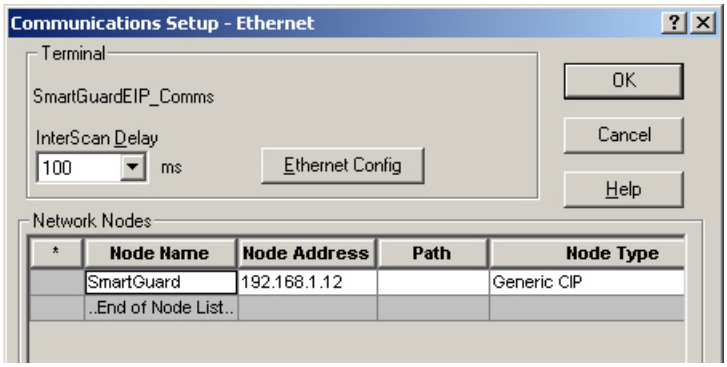
2. Klicken Sie auf „Communications Setup“ (Kommunikation konfigurieren).

   Das Dialogfeld „Communications Setup – Ethernet“ (Kommunikation konfigurieren – Ethernet) wird angezeigt.

3. Klicken Sie auf „Insert“ (Einfügen).

4. Geben Sie den Netzknotennamen und die Netzknotenadresse der SmartGuard-Steuerung ein.

5. Geben Sie als Netzknotentyp „Generic CIP“ (Generisches CIP) ein.



6. Klicken Sie auf „OK“.

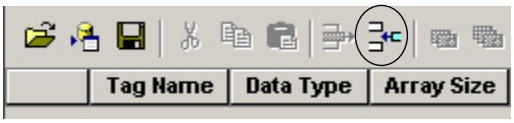
Gehen Sie wie folgt vor, um Tags in der PanelView-Tag-Datenbank zu definieren, die auf die Ziel-E/A-Baugruppen in der SmartGuard 600-Steuerung zugreift.

1. Klicken Sie im Anwendungs-Explorer auf „Tag Editor“ (Tag-Editor).

   Der Tag-Editor der Anwendung wird geöffnet.

2. Klicken Sie am unteren Rand des Tag-Editors auf die Registerkarte „ENet-CIP“.

3. Klicken Sie auf „Insert“ (Einfügen), um ein neues Tag hinzuzufügen.



4. Geben Sie in die neuen Tag-Zellen den Tag-Namen, einen Datentyp und den Netzknotennamen ein (dieser muss mit dem Netzknotennamen übereinstimmen, den Sie für die SmartGuard-Steuerung in der Kommunikationskonfiguration definiert haben).

   In diesem Beispiel wird DINT als Datentyp angegeben.

	Tag Name	Data Type	Descrip	Node Name
1	SG_InputAssembly	DINT		SmartGuard

In der SmartGuard-Steuerung können bis zu vier Ziel-E/A-Baugruppen konfiguriert werden (zwei Eingänge und zwei Ausgänge).

Für Eingangsbaugruppen umfassen die CIP-Nachrichtencodes Folgendes:

- Service: 0xE – Get Single Attribute (Einzelnes Attribut abrufen)
- Class (Klasse): 4
- Instance (Instanz): 100 oder 101 (Eingang 1 oder Eingang 2)
- Attribute (Attribut): 3

Für Ausgangsbaugruppen umfassen die CIP-Nachrichtencodes Folgendes:

- Service: 0x10 – Set Single Attribute (Einzelattribut festlegen)
- Class (Klasse): 4
- Instance (Instanz): 102 oder 103 (Ausgang 1 oder Ausgang 2)
- Attribute (Attribut): 3

Dieses Beispiel zeigt einen CIP-Nachrichtencode, der auf Eingangsbaugruppe 1 der SmartGuard-Steuerung zugreift.

Im Feld „Member“ (Glied) ist stets der Wert 1 definiert.

1. Wählen Sie im Pulldown-Menü „Service Code“ den CIP-Dienstcode aus.

2. Geben Sie die Klassen-, Instanz- und Attributcodes für das Tag ein, um auf die richtigen Ziel-E/A-Baugruppen in der SmartGuard-Steuerung zugreifen zu können.

	Tag Name	Data Type	Descrip	Node Name	Initial Value	Array Size	Service Code	Class	Instance	Attribute	Member	Byte Offset
1	SG_InputAssembly	DINT		SmartGuard	0	0	Get Attribute Single (0xE)	4	100	3	1	0

Die maximale Größe eines einzelnen Member-Tags, das im PanelView-Terminal definiert ist, entspricht einem DINT (4 Bytes). Eine Ziel-E/A-Baugruppe in der SmartGuard-Steuerung kann bis zu 16 Bytes groß sein. Um auf alle Bytes in der Zielbaugruppe zugreifen zu können, müssen Sie möglicherweise bis zu 4 DINT-Tags erzeugen, wobei für jedes Tag ein Offset definiert wird, damit es den Ziel-Bytes dieses Tags entspricht.

Einrichten der Steuerungsmodi

Einleitung

Thema	Seite
Einrichten des automatischen Ausführungsmodus (optional)	139
Einrichten des eigenständigen Kommunikationsmodus (optional)	140
Ändern des Modus einer Steuerung	142

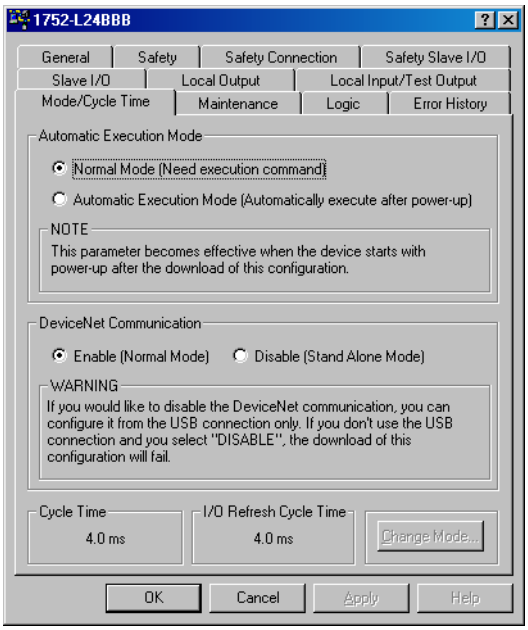
Einrichten des automatischen Ausführungsmodus (optional)

Die Steuerung kann für den Modus „Normal“ oder „Automatic Execution“ konfiguriert werden. Der automatische Ausführungsmodus sollte erst im Anschluss an die Konfiguration des Systems eingerichtet werden. Die Einstellung wird wirksam, nachdem Sie im Anschluss an einen Konfigurationsdownload das Gerät aus- und eingeschaltet haben.

Führen Sie folgende Schritte durch, um den Modus einzurichten.

1. Klicken Sie mit der rechten Maustaste auf die Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

2. Wählen Sie die Registerkarte „Mode/Cycle Time“ (Modus/Zykluszeit) aus.



3. Wählen Sie entweder „Normal Mode“ (Normaler Modus) oder „Automatic Execution Mode“ (Automatischer Ausführungsmodus) aus.

Modus	Beschreibung
Normal	Die Steuerung wird beim Einschalten im Modus „Idle“ (Leerlauf) gestartet. Sie müssen RSNetWorx for DeviceNet verwenden, um in den Modus „Execute“ (Ausführen) zu wechseln, indem Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf der Registerkarte „Mode/Cycle Time“ (Modus/Zykluszeit) auf „Change Mode“ (Modus ändern) klicken.
Automatische Ausführung	Die Steuerung startet beim Einschalten im Modus „Execute“ (Ausführen), sofern die Konfiguration gesperrt wurde und sich die Steuerung vor dem Ausschalten im Modus „Execute“ befand.

4. Klicken Sie auf „OK“.

Einrichten des eigenständigen Kommunikationsmodus (optional)

Die SmartGuard-Steuerung kann mit aktivierter oder ohne aktivierte DeviceNet-Kommunikation betrieben werden. In der Standardeinstellung ist diese aktiviert.

Im eigenständigen Modus ist die Zykluszeit der Steuerung kürzer, es kann jedoch keine der DeviceNet-Kommunikationsfunktionen verwendet werden.

Wenn die SmartGuard-Steuerung im eigenständigen Modus verwendet werden soll, kann die DeviceNet-Kommunikation deaktiviert und zur Konfiguration des Moduls eine USB-Verbindung verwendet werden.

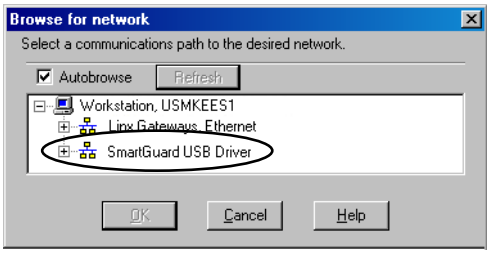
WICHTIG Wenn die DeviceNet-Kommunikation deaktiviert wird und Sie die USB-Verbindung nicht verwenden, kann die Konfiguration nicht heruntergeladen werden.

Führen Sie folgende Schritte durch, um die DeviceNet-Kommunikation zu deaktivieren.

1. Stellen Sie sicher, dass Sie über die USB-Verbindung mit dem Programmiergerät verbunden sind.

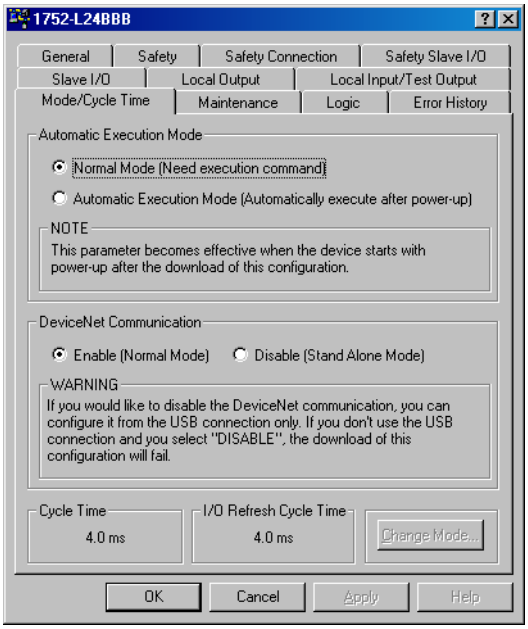
2. Richten Sie gegebenenfalls einen Pfad für die Verwendung der USB-Verbindung in RSNetWorx for DeviceNet ein.
   a. Wählen Sie im Menü „Network“ (Netzwerk) die Option „Properties“ (Eigenschaften) aus.
   b. Klicken Sie im Dialogfeld „DeviceNet“ auf „Set Online Path“ (Online-Pfad festlegen).

c. Wählen Sie im Dialogfeld „Browse for Network“ (Nach Netzwerk suchen) den gewünschten Pfad aus, und klicken Sie auf „OK“.



3. Klicken Sie in RSNetWorx for DeviceNet mit der rechten Maustaste auf die Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

4. Wählen Sie die Registerkarte „Mode/Cycle Time“ (Modus/Zykluszeit) aus.



5. Wählen Sie „Disable (Stand Alone Mode)“ (Deaktivieren (Eigenständiger Modus)) aus, und klicken Sie auf „OK“.

Ändern des Modus einer Steuerung

Führen Sie folgende Schritte durch, um den Modus einer Steuerung zu ändern.

1. Gehen Sie mit der SmartGuard-Steuerung online.
2. Klicken Sie mit der rechten Maustaste auf die Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.
3. Wählen Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) die Registerkarte „Mode/Cycle Time“ (Modus/Zykluszeit) aus.
4. Klicken Sie auf „Change Mode“ (Modus ändern).
5. Wählen Sie das Optionsfeld „Idle“ (Leerlauf) oder „Execute“ (Ausführen) aus.
6. Klicken Sie auf „OK“.

Erstellen eines Anwendungsprogramms

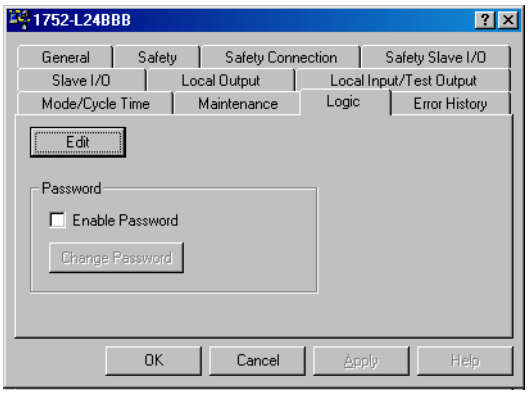
Einleitung

Thema	Seite
Der Logik-Editor	143
Grundlagen der Programmierung	144
Erstellen eines Funktionsblockprogramms	149
Bearbeiten von Funktionsblockparametern	150
Suchen von Funktionsblöcken mit offenen Verbindungen	153
Programmieren auf mehreren Seiten	154
Speichern des Programms	155
Aktualisieren des Programms	155
Online-Überwachung des Programms	156
Abfolge der Programmausführung	157
Benutzerdefinierte Funktionsblöcke	158
Zusätzliche Hilfsmittel	163

Der Logik-Editor

Die SmartGuard 600-Steuerung wird mit dem Logik-Editor in der Software RSNetWorx for DeviceNet programmiert. Der Logik-Editor enthält eine Objektliste, in der Funktionsblöcke, E/A-Tags und andere Programmierelemente erfasst sind, sowie einen Arbeitsbereich, in dem die Programmierung erfolgt.

Sie öffnen den Logik-Editor, indem Sie im Dialogfeld „Edit Device Parameters“ (Geräteparameter bearbeiten) auf der Registerkarte „Logic“ (Logik) auf „Edit“ (Bearbeiten) klicken.



Sie können das Anwendungsprogramm durch ein Kennwort schützen, um das nicht autorisierte Bearbeiten, Überprüfen oder Drucken von Programmen zu verhindern. Gehen Sie zum Erstellen eines Kennworts folgendermaßen vor.

1. Aktivieren Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf der Registerkarte „Logic“ (Logik) das Kontrollkästchen „Enable Password“ (Kennwort aktivieren).

2. Geben Sie im Dialogfeld „Change Password“ (Kennwort ändern) im Feld „New Password“ (Neues Kennwort) das Kennwort ein.

   Kennwörter dürfen maximal sechs Zeichen enthalten.

3. Geben Sie das Kennwort im Feld „Confirm Password“ (Kennwort bestätigen) erneut ein.

4. Klicken Sie auf „OK“.

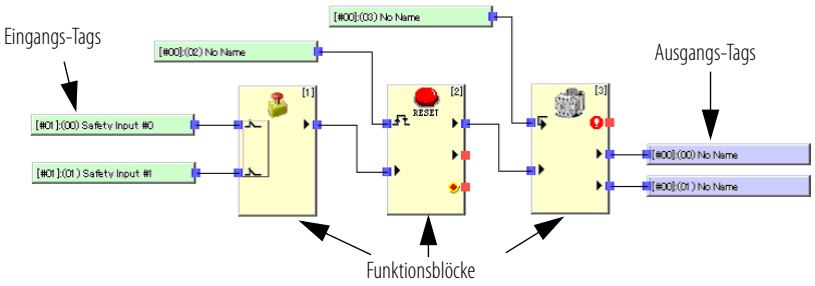
Das Kennwort wird immer dann abgefragt, wenn auf die Schaltfläche „Edit“ (Bearbeiten) geklickt wird, um den Logik-Editor zu öffnen. Sie können das Programm ohne Kennwort hoch- und herunterladen, Funktionen zum Bearbeiten, Überprüfen, Drucken und zum Erstellen von Berichten sind jedoch nicht verfügbar.

WICHTIG Wenn Sie das Kennwort vergessen, kann es nicht wiederhergestellt werden.

Grundlagen der Programmierung

Das Erstellen von Programmen erfolgt mit logischen Funktionsblöcken, die Befehle angeben, mit Eingangs-Tags, die Dateneingangsquellen angeben, und mit Ausgangs-Tags, die Ziele für die Datenausgabe angeben. Die Ein- und Ausgänge werden mit Verbindungslinien verbunden.

E/A-Verbindungen



Logische Funktionen und Funktionsblöcke

Es können maximal 254 logische Funktionen und Funktionsblöcke verwendet werden.

Unterstützte logische Befehle und Funktionsblöcke

Logische Befehle	Funktionsblöcke
• NOT (Logisches Nicht) • AND (Logische Und-Operation) • OR (Logisches Oder) • Exklusive OR (Exklusives Oder) • Exklusive NOR (Exklusives Nicht-Oder) • Routing • RS Flip-Flop • Multi Connector (Mehrfachverbindungspunkt) • Comparator (Vergleicher)	• Reset • Restart • Überwachung Not-Aus-Taster • Überwachung Lichtgitter • Überwachung Sicherheitstür • 2-Hand-Steuerung • Ausschaltverzögerter Timer • Einschaltverzögerter Timer • Anwendermodus-Schalter • Externe Geräteüberwachung • Muting • Zustimmschalter • Impulsgeber • Zähler

Eingangs-Tags

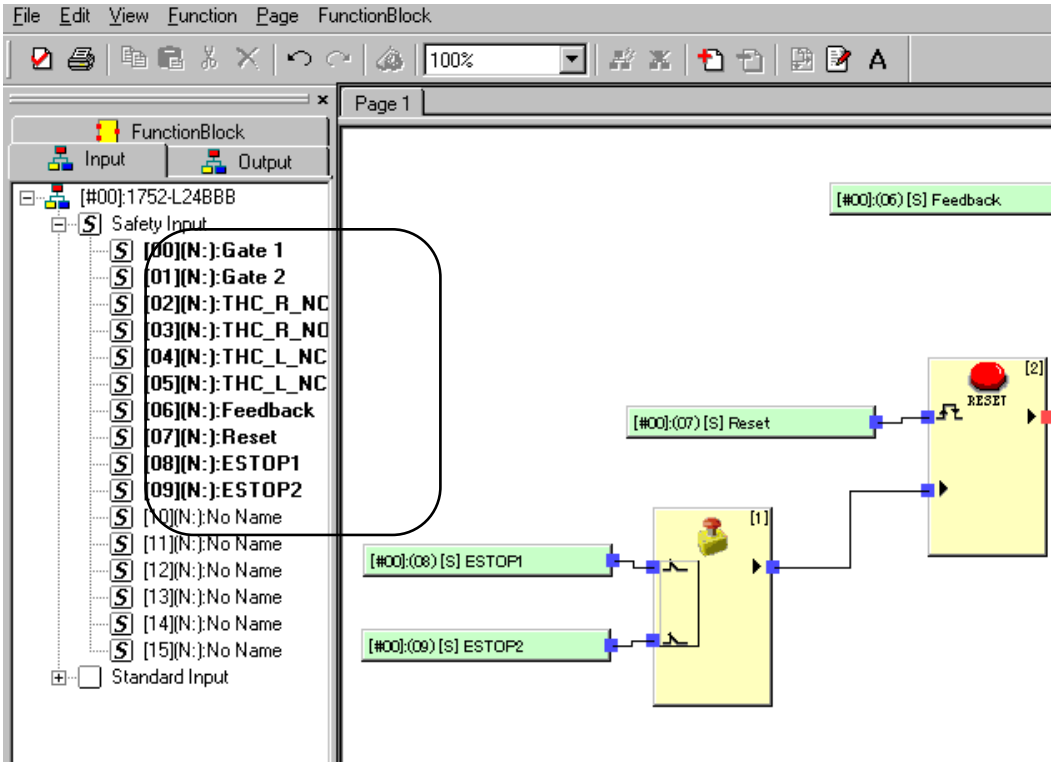
Eingangs-Tags geben den Status der Eingänge folgender E/A-Bereiche an:

- Zentrale Anschlüsse der Steuerung
- Eingangsbereich der als Kommunikationspartner registrierten Sicherheits-Slaves
- Von den Daten des Sicherheits-Masters reflektierter Eingangsbereich
- Von den Daten des Standard-Masters reflektierter Eingangsbereich

Daten werden in folgenden E/A-Bereichen reflektiert:

- Status zentraler Eingang
- Status zentraler Ausgang
- Allgemeiner Gerätestatus
- Status Testausgang
- Status Muting-Lampe

E/A-Tags werden in der Objektliste mit Symbolen angezeigt, die über ihre Konfiguration Aufschluss geben.

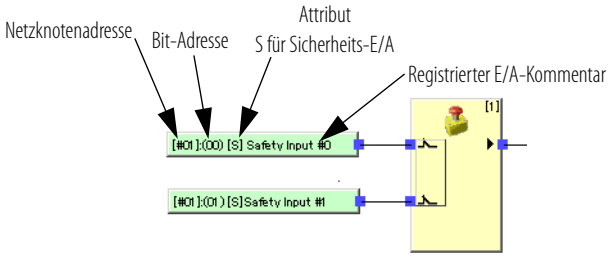


Symbole für Eingangs-Tags

Eingangsart	Symbol	Kanalmodus	Symbol
Nicht verwendet	N	Einzeln	Kein
Testimpuls vom Testausgang	P	Zweikanal-Äquivalent	e
Verwendung als Sicherheitseingang	S	Zweikanal-Komplement	c
Verwendung als Standardeingang	ST	–	

Bei der Verwendung im Arbeitsbereich beinhalten Eingangs-Tags Netzknotenadresse, Bit-Adresse, Attribut (S für Sicherheit, kein Attribut bei Standard) und registrierten E/A-Kommentar.

Eingangs-Tags



Ausgangs-Tags

Ausgangs-Tags geben den Status der Ausgänge folgender E/A-Bereiche an:

- Zentrale Anschlüsse der Steuerung
- Ausgangsbereich der als Kommunikationspartner registrierten Sicherheits-Slaves
- Von den Daten des Sicherheits-Masters reflektierter Ausgangsbereich
- Von den Daten des Standard-Masters reflektierter Ausgangsbereich

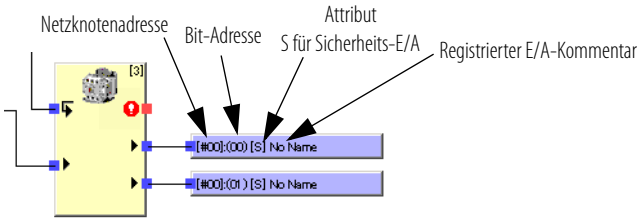
E/A-Tags werden in der Objektliste mit Symbolen angezeigt, die über ihre Konfiguration Aufschluss geben.

Symbole für Ausgangs-Tags

Ausgangsart	Symbol	Kanalmodus	Symbol
Nicht verwendet	N	Einzeln	Kein
Sicherheit	S	Dual	d
Sicherheitsimpulstest	P	–	

Bei der Verwendung im Arbeitsbereich beinhalten Ausgangs-Tags Netzknotenadresse, Bit-Adresse, Attribut (S für Sicherheit, kein Attribut bei Standard) und registrierten E/A-Kommentar.

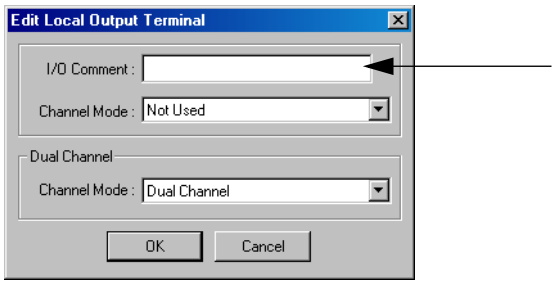
Ausgangs-Tags



E/A-Kommentarfunktion

Der E/A-Kommentar ist ein optionaler Name, der bis zu 32 ASCII-Zeichen enthalten darf und in der Steuerung mittels RSNetWorx for DeviceNet für jeden E/A-Anschluss registriert werden kann. Sie können diese E/A-Kommentare in der Objektliste des Logik-Editors als E/A-Tags verwenden, um die Programmierung zu vereinfachen.

E/A-Kommentar



Einschränkungen bei der Programmierung

Elemente wie E/A-Tags und Funktionsblöcke können mit folgenden Einschränkungen auf sämtlichen Seiten verwendet werden:

- Dasselbe Eingangs-Tag darf auf mehreren Seiten verwendet werden.
- Dasselbe Eingangs-Tag darf auf jeder Seite nur einmal verwendet werden.
- Jedes Ausgangs-Tag darf nur einmal im Anwendungsprogramm verwendet werden.
- Nur Funktionsblöcke können kopiert werden. E/A-Tags, E/A-Tag-Verbindungen und Verbindungen zwischen Funktionsblöcken können nicht kopiert werden.
- Ein Funktionsblock wird an derselben Position eingefügt wie der kopierte Funktionsblock. Wenn Sie einen Funktionsblock auf derselben Seite einfügen, wird damit der Quellfunktionsblock verschoben.
- Es können maximal 254 Funktionsblöcke verwendet werden.
- Es können maximal 128 Sprungadressen für Zahlen verwendet werden.
- Es können maximal 32 Seiten verwendet werden.
- Es können maximal 128 Textfelder für Programmkommentare verwendet werden.
- Die Seiteneinrichtung darf nicht geändert werden, wenn der Arbeitsbereich Elemente enthält. Legen Sie die Größe des Arbeitsbereichs im Vorfeld unter „File > Page Setup“ (Datei > Seite einrichten) fest.

Erstellen eines Funktionsblockprogramms

Für das Erstellen eines Programms mit Funktionsblöcken erstellen Sie Verbindungen vom Funktionsblock zu den Eingangs- und Ausgangs-Tags.

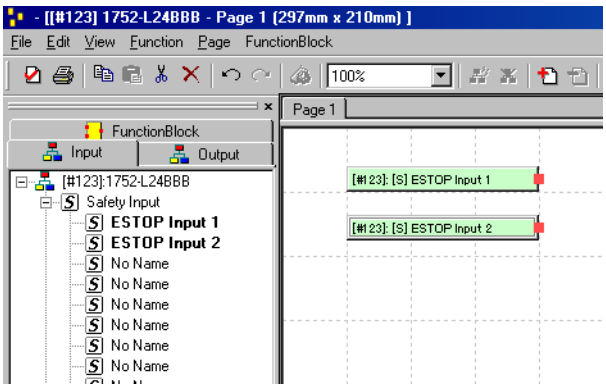
Hinzufügen eines Eingangs- oder Ausgangs-Tags

Gehen Sie zum Hinzufügen eines Tags folgendermaßen vor.

1. Klicken Sie in der Objektliste auf die Registerkarte „Input“ (Eingang) oder „Output“ (Ausgang).
2. Wählen Sie das zu verwendende Tag aus, und ziehen Sie es per Drag & Drop an die gewünschte Position im Arbeitsbereich.

   Sie können mehrere E/A-Tags gleichzeitig auswählen und positionieren.

Positionieren von Eingangs-Tags



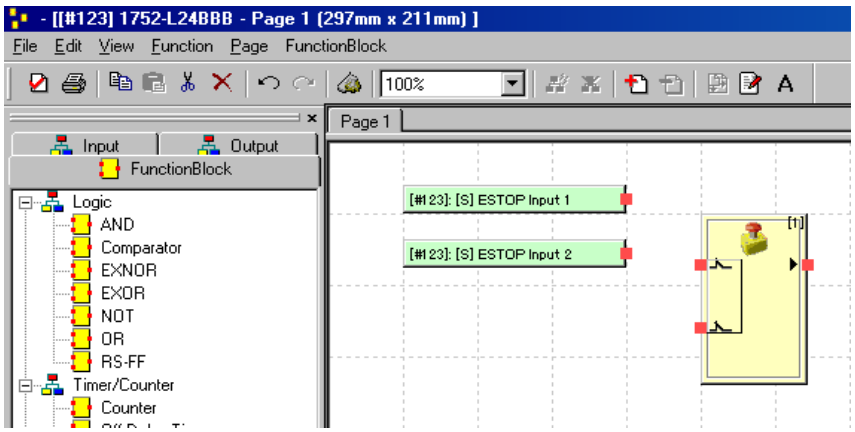
TIPP Die im Anwendungsprogramm verwendeten Eingangs- und Ausgangs-Tags werden in der Objektliste fett formatiert.

Hinzufügen eines Funktionsblocks

Gehen Sie zum Hinzufügen eines Funktionsblocks zum Arbeitsbereich folgendermaßen vor.

1. Klicken Sie in der Objektliste auf die Registerkarte „Function Block“.
2. Wählen Sie den zu verwendenden Funktionsblock aus, und ziehen Sie ihn per Drag & Drop an die gewünschte Position im Arbeitsbereich.

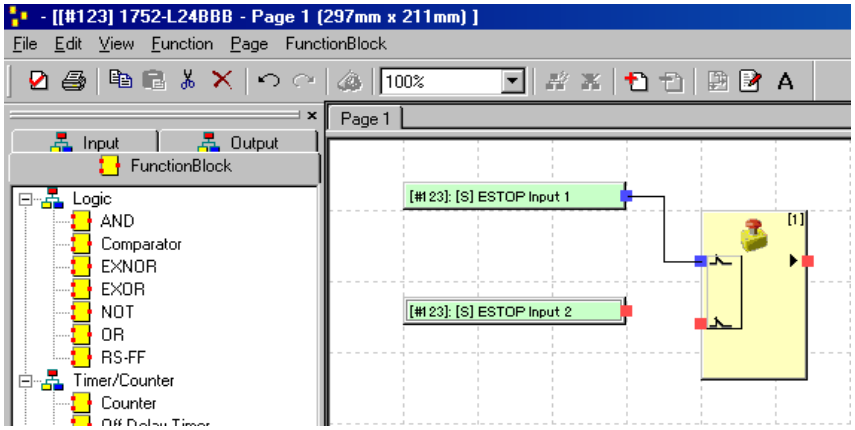
Positionieren eines Funktionsblocks



Verbinden der Tags mit dem Funktionsblock

Klicken Sie zum Verbinden der E/A-Tags mit dem Funktionsblock auf den Quellverbindungspunkt (■), und ziehen Sie diesen zum Zielverbindungspunkt (■).

Verbinden von Tags mit Funktionsblöcken

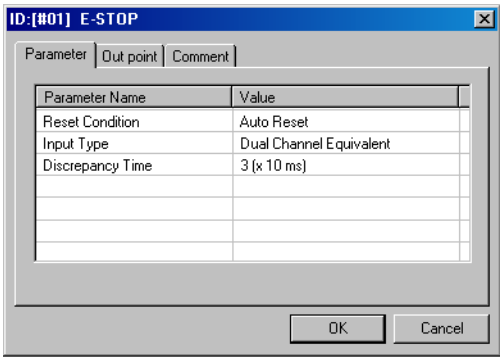


Bearbeiten von Funktionsblockparametern

Sie können Funktionsblöcke bearbeiten, indem Sie die Parametereinstellungen ändern, die Anzahl der Ein- oder Ausgänge ändern, optionale E/A hinzufügen und Kommentare zur Anwendung einfügen. Die Parameter, die Sie bearbeiten können, sind vom Typ des Funktionsblocks abhängig.

Klicken Sie zum Öffnen des Dialogfelds „Function Block Properties“ (Eigenschaften des Funktionsblocks) mit der rechten Maustaste auf den Funktionsblock und anschließend auf „Edit“ (Bearbeiten).

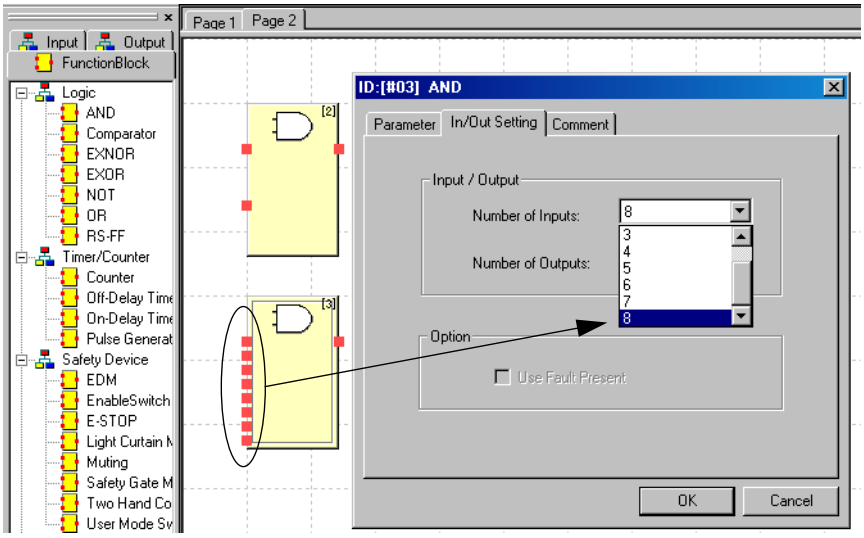
Registerkarte „Parameter“



Ein-/Ausgangseinstellungen

Sie können die Anzahl der Eingänge und Ausgänge sowie in einigen Fällen auch die Fehlereinstellungen für viele Befehle bearbeiten.

Registerkarte „In/Out Setting“ (E/A-Einstellungen)



Number of Inputs (Anzahl der Eingänge)

Sie können die Anzahl der Eingänge für logische Funktionen erhöhen oder den optionalen Eingang für Funktionsblöcke aktivieren.

Number of Outputs (Anzahl der Ausgänge)

Sie können die Anzahl der Ausgänge für logische Funktionen erhöhen oder die optionalen Ausgänge, z. B. Fehlerausgänge, von Funktionsblöcken aktivieren.

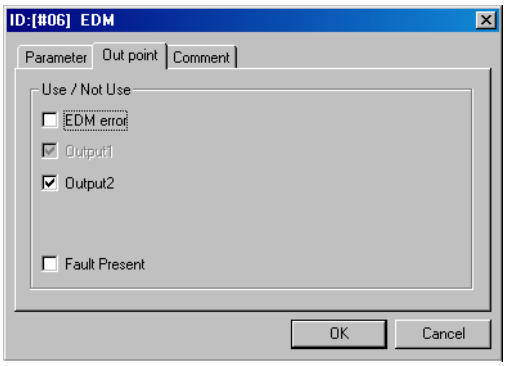
Fault Present Bit (Fehlerbit)

Sie können das Diagnose-Status-Bit für Fehler in einigen Funktionsblöcken aktivieren, indem Sie im Dialogfeld „Function Block Properties“ (Funktionsblockeigenschaften) auf der Registerkarte „In/Out Setting“ (E/A-Einstellungen) das Kontrollkästchen aktivieren. Wenn das Kontrollkästchen „Use Fault Present“ (Vorhandenen Fehler verwenden) aktiviert ist, wird im Funktionsblock der zusätzliche Ausgang „Fault Present“ angezeigt.

Optionale Ausgangspunktauswahl

Sie können optionale Ausgänge aktivieren, einschließlich „Fault Present“-Bit für einige Funktionsblöcke, indem Sie im Dialogfeld „Function Block Properties“ (Funktionsblockeigenschaften) auf der Registerkarte „Out point“ (Ausgangspunkt) die entsprechenden Kontrollkästchen aktivieren. Wenn die optionalen Ausgänge aktiviert sind, werden sie im Funktionsblock angezeigt.

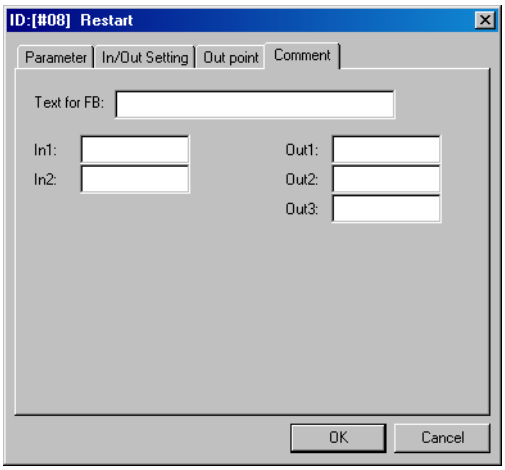
Registerkarte „Out point“ (Ausgangspunkt)



Kommentare

Auf der Registerkarte „Comments“ (Kommentare) können Sie einen Namen für den Funktionsblock oder für E/A-Signale eingeben. Die Namen von E/A-Signalen werden im Arbeitsbereich nicht angezeigt, der Name des Funktionsblocks wird hingegen im Arbeitsbereich unterhalb des Funktionsblocks angezeigt. Alle in diesem Dialogfeld eingegebenen Namen werden beim Drucken des Anwendungsprogramms ebenfalls gedruckt.

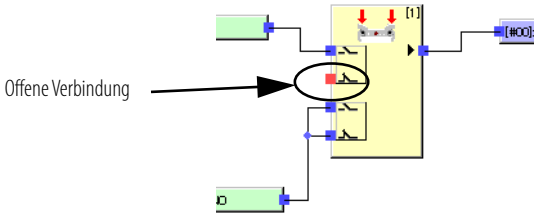
Registerkarte „Comment“ (Kommentar)



Suchen von Funktionsblöcken mit offenen Verbindungen

Neu erstellte Programme, die Funktionsblöcke mit offenen Eingängen oder Ausgängen enthalten, können nicht heruntergeladen werden. Alle Ein- und Ausgänge müssen verwendet werden.

Funktionsblock mit offenen Verbindungen



Wählen Sie im Logik-Editor zum Suchen aller offenen Verbindungen „Edit > Search OpenConnection“ (Bearbeiten > Offene Verbindung suchen) aus.

Im Dialogfeld „Open Connection“ (Offene Verbindung) werden sämtliche Funktionsblöcke mit offenen Verbindungen angezeigt. Doppelklicken Sie auf ein Element in der Liste, um den Funktionsblock anzuzeigen. Offene Verbindungen werden im Arbeitsbereich rot angezeigt.

TIPP

Wenn für den E/A-Punkt eine Sprungadresse verwendet wird, die zugehörige Sprungadresse jedoch nicht verwendet wird, wird der E/A-Punkt nicht rot angezeigt, sondern so dargestellt, als bestünde eine Verbindung.

Weitere Informationen über Sprungadressen finden Sie im Abschnitt Programmieren auf mehreren Seiten auf Seite 154.

Programmieren auf mehreren Seiten

Die SmartGuard 600-Steuerung unterstützt bis zu 32 Seiten Programmierlogik.

Klicken Sie zum Erstellen einer neuen Seite auf das Symbol „Add Page“ (Seite hinzufügen).

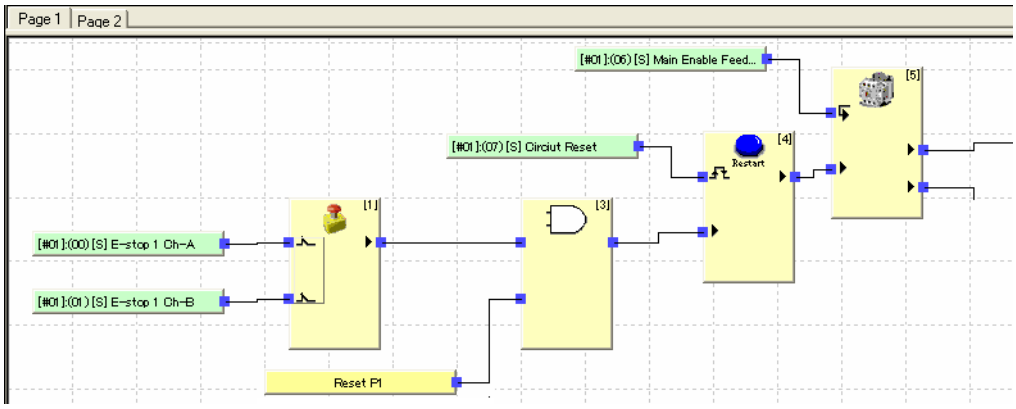
Verwenden Sie zum Verbinden der Logik auf verschiedenen Seiten Sprungadressen. Ein Programm für die SmartGuard 600-Steuerung kann bis zu 128 Sprungadressen enthalten.

Gehen Sie zum Erstellen einer Sprungadresse folgendermaßen vor.

1. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle auf der Programmierseite, und wählen Sie „Make JumpAddress“ (Sprungadresse erstellen) aus.

2. Geben Sie einen Namen für die Sprungadresse ein.

3. Verbinden Sie die Sprungadresse mit dem Funktionsblock.

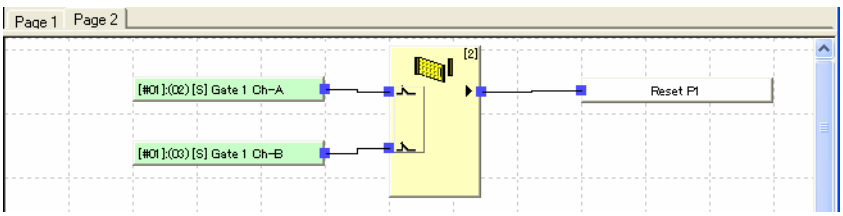


4. Wählen Sie die Seite aus, mit der Sie die Logik verbinden möchten.

5. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle auf der Seite, und wählen Sie „Select JumpAddress“ (Sprungadresse auswählen) aus.

6. Wählen Sie die Sprungadresse aus dem Pulldown-Menü aus.

7. Verbinden Sie die Sprungadresse mit dem Funktionsblock.



Speichern des Programms

Gehen Sie zum Speichern des Anwendungsprogramms folgendermaßen vor.

1. Wählen Sie „File > Apply“ (Datei > Übernehmen) aus.

   Das Programm wird zeitweilig in RSNetWorx for DeviceNet gespeichert.

2. Beenden Sie Logik-Editor durch Auswahl von „File > Exit“ (Datei > Beenden).

3. Klicken Sie im Dialogfeld „Edit Device Parameters“ (Geräteparameter bearbeiten) auf „OK“ oder „Apply“ (Übernehmen).

   Wenn Sie nicht auf „OK“ oder „Apply“ (Übernehmen) klicken oder wenn Sie auf „Cancel“ (Abbrechen) klicken, werden keine Programmänderungen gespeichert. Sämtliche Programmänderungen, die zeitweilig mit „File > Apply“ (Datei > Übernehmen) gespeichert wurden, werden gelöscht.

4. Wählen Sie im Hauptdialogfeld von RSNetWorx for DeviceNet „Save“ (Speichern) oder „Save As“ (Speichern unter) aus.

Aktualisieren des Programms

Wenn die E/A-Tags von Sicherheits-Slaves, die die zentralen Ein- und Ausgänge der SmartGuard-Steuerung konfigurieren, geändert werden, müssen Sie den Logik-Editor starten und das Programm überprüfen.

Wenn Sie die Parameter auf die Steuerung laden, ohne den Logik-Editor zu starten, tritt beim Herunterlade ein Fehler im Logik-Editor auf, da die Daten inkonsistent sind. Wenn dieser Fehler auftritt, starten Sie den Logik-Editor und überprüfen das Programm. Nehmen Sie ggf. erforderliche Änderungen vor.

Online-Überwachung des Programms

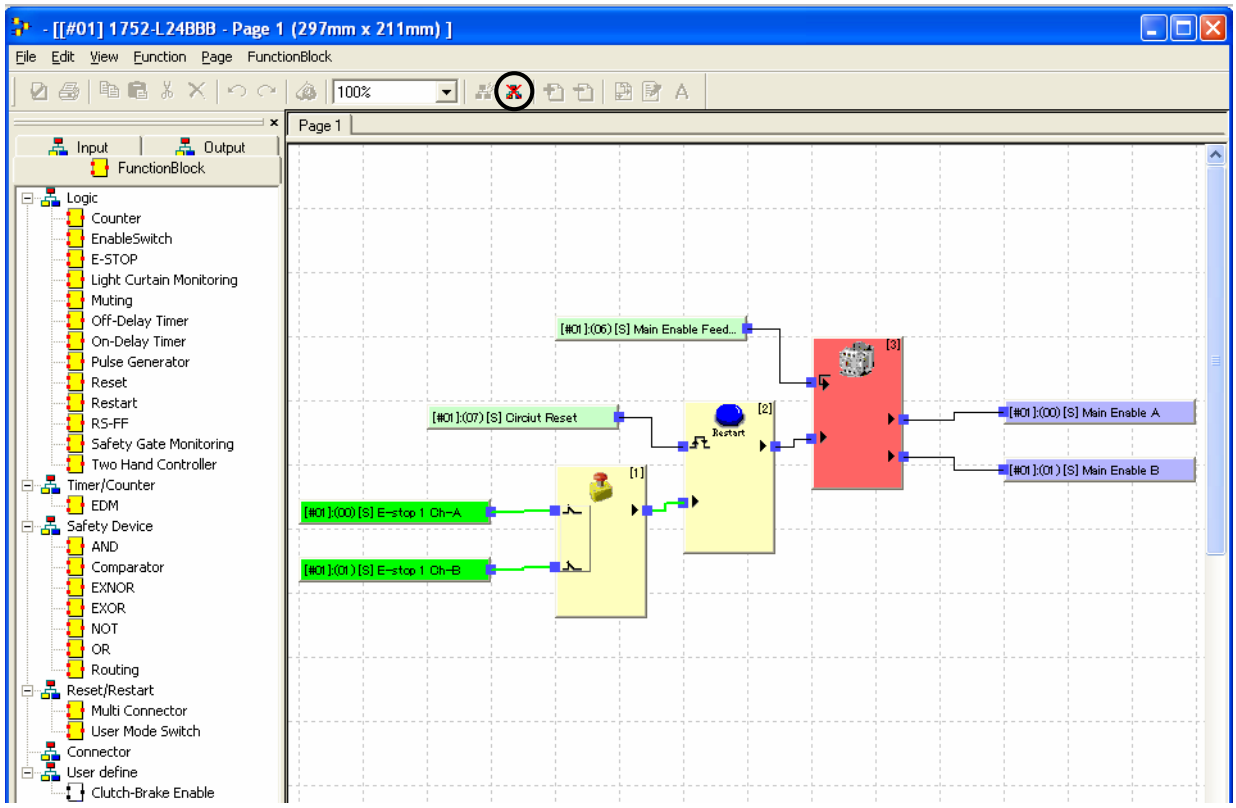
Sie können die Werte der E/A-Tags und die Signalzustände von Verbindungen mit Funktionsblöcken online im Logik-Editor überwachen. Stellen Sie sicher, dass RSNetWorx for DeviceNet mit dem Netzwerk verbunden ist und dass die überwachte Steuerung im Betriebsmodus „Run“ (Betrieb) ist, bevor Sie die Online-Überwachung des Programms starten.

WICHTIG Sie müssen möglicherweise den Betriebsmodus der Steuerung in „Execute“ (Ausführen) ändern, um die Online-Überwachung durchführen zu können.

Klicken Sie zum Starten der Online-Überwachung auf der Symbolleiste auf „Monitoring“ (Überwachen) .

Während der Überwachung werden E/A-Tags oder Verbindungen, die in Betrieb sind, in einer dunkleren Farbe dargestellt.

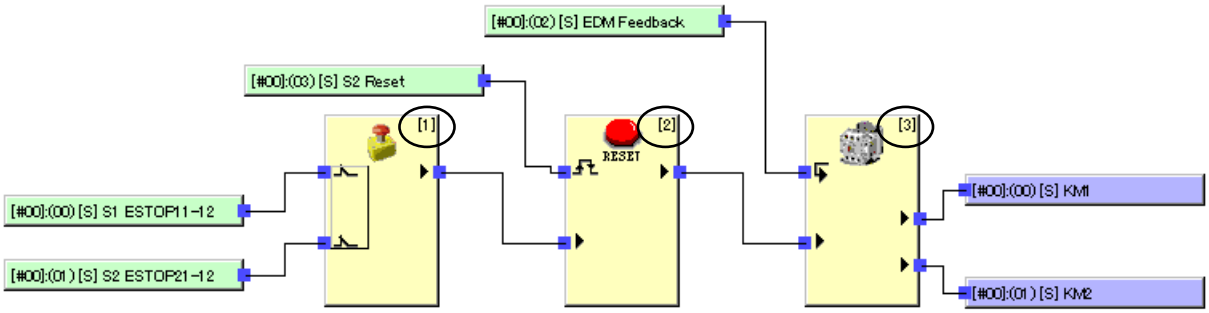
Klicken Sie zum Beenden der Online-Überwachung auf der Symbolleiste auf „Stop Monitoring“ (Überwachung beenden).



Abfolge der Programmausführung

Die Ausführungsreihenfolge von Funktionsblocken wird automatisch vom Logik-Editor festgelegt und in der rechten Ecke der einzelnen Funktionsblöcke angezeigt.

Beispielprogramm

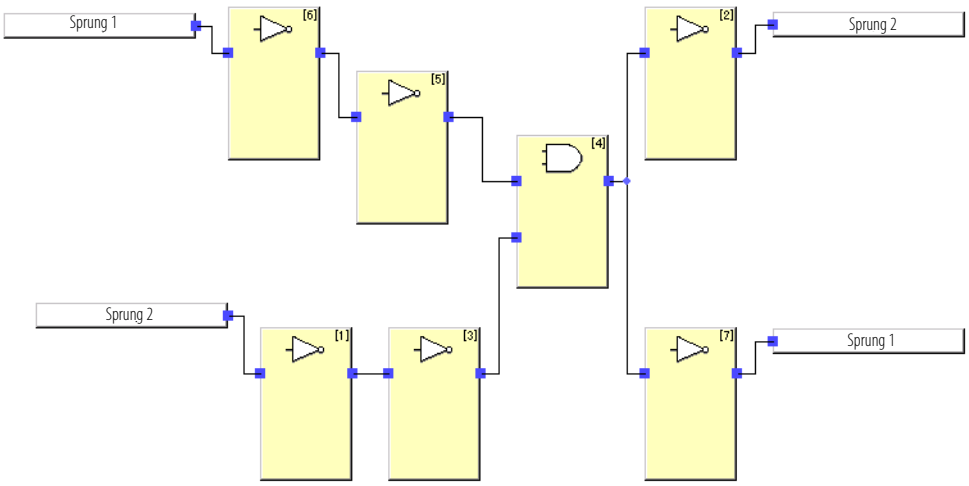


In diesem Beispiel lautet die Ausführungsreihenfolge:

1. E-Stop (Not-Aus)
2. Reset
3. External Device Monitoring – EDM (Externe Geräteüberwachung)

Mithilfe von Sprungadressen können Sie in Programmen Schleifen erstellen. Wenn ein Programm mehrere Schleifen enthält, z. B. von Sprung 1 zu Sprung 1 und Sprung 2 zu Sprung 2, entspricht die Ausführungsreihenfolge der Reihenfolge, in der die Funktionsblöcke angeordnet sind. Testen Sie sämtliche Programme mit mehreren Schleifen sehr sorgfältig, um deren ordnungsgemäße Ausführung sicherzustellen.

Beispielschleife



Benutzerdefinierte Funktionsblöcke

Sie können im Logik-Editor benutzerdefinierte Funktionsblöcke erstellen, die Logik aus vorhandenen Funktionsblöcken enthalten. Nach dem Erstellen werden diese Funktionsblöcke in einer benutzerdefinierten Bibliothek gespeichert und können in allen Anwendungen für die SmartGuard-Steuerung verwendet werden.

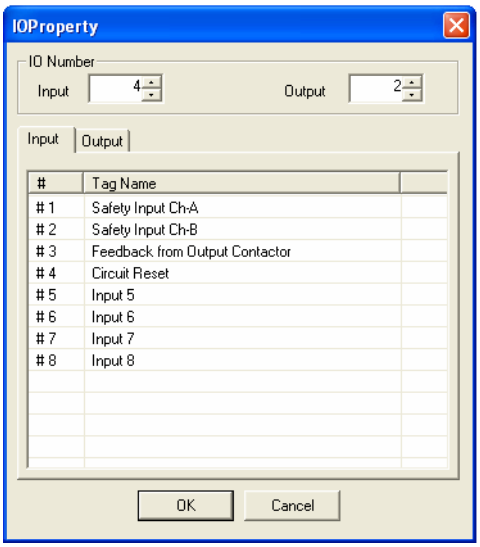
Erstellen von benutzerdefinierten Funktionsblöcken

Gehen Sie zum Erstellen eines benutzerdefinierten Funktionsblocks folgendermaßen vor.

1. Öffnen Sie den Logik-Editor, indem Sie mit der rechten Maustaste auf die Steuerung klicken, wählen Sie „Properties“ (Eigenschaften) aus, und klicken Sie auf der Registerkarte „Logic“ (Logik) auf „Edit“ (Bearbeiten).

2. Wählen Sie „FunctionBlock > Create“ (Funktionsblock > Erstellen) aus.

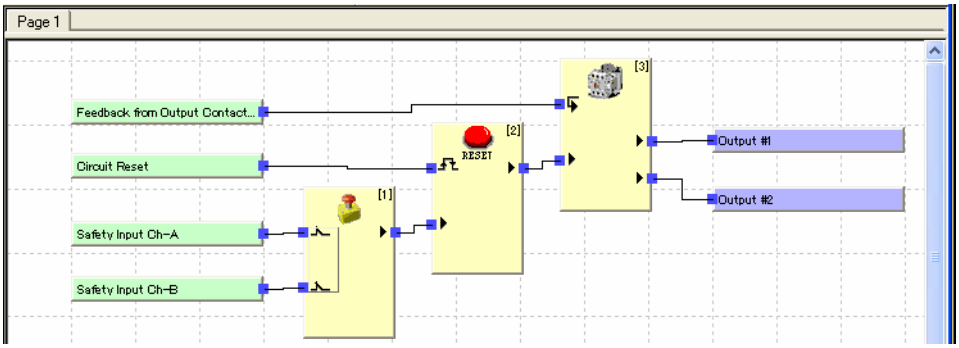
3. Definieren Sie im Dialogfeld „IOProperty“ (E/A-Eigenschaften) die Anzahl der Ein- und Ausgänge für den Funktionsblock.



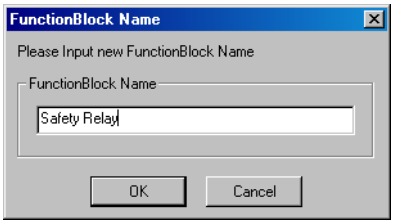
4. Weisen Sie den einzelnen Ein- und Ausgängen Namen zu.

5. Klicken Sie auf „OK“, um den Logik-Editor für den Funktionsblock zu öffnen.

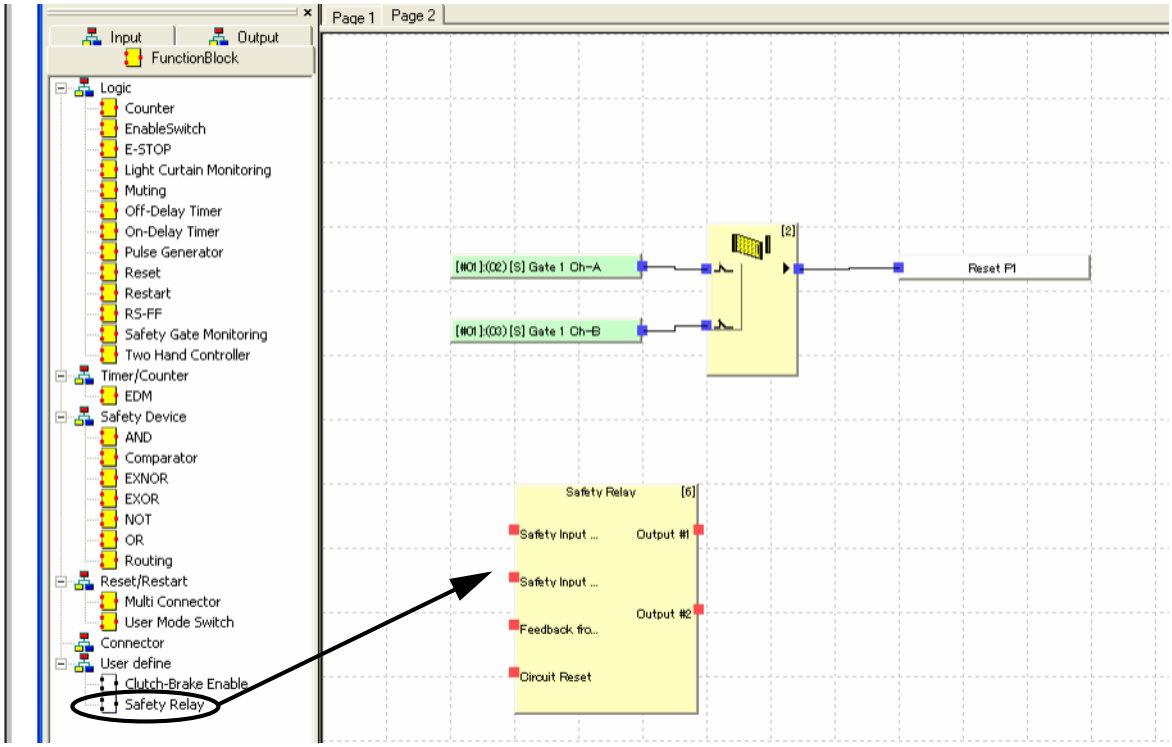
6. Schreiben Sie die Logik für den Funktionsblock.



7. Wählen Sie „File > Save“ (Datei > Speichern), und geben Sie einen Namen für den Funktionsblock ein, wenn Sie dazu aufgefordert werden.



8. Fügen Sie den neuen Funktionsblock zur Anwendungslogik hinzu.



TIPP

Wenn Sie den benutzerdefinierten Funktionsblock bearbeiten möchten, kann dieser in der derzeitigen Anwendung nicht verwendet werden. In diesem Fall ist die Option für die Bearbeitung nicht verfügbar.

WICHTIG Bevor Sie Programme mit benutzerdefinierten Funktionsblöcken in einer Anwendung verwenden, sollten Sie sie immer auf die Steuerung herunterladen und ihre Konfiguration und Funktion überprüfen.

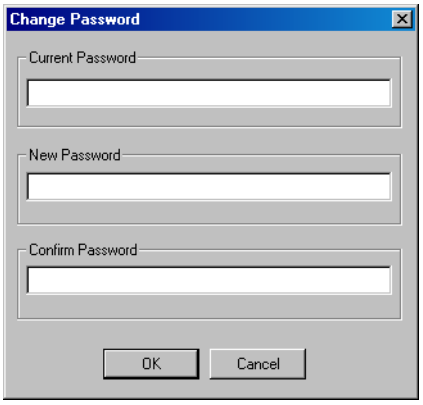
Schützen von benutzerdefinierten Funktionsblöcken durch ein Kennwort

Sie können ein Kennwort festlegen, um Dateien mit benutzerdefinierten Funktionsblöcken vor einer nicht autorisierten Bearbeitung zu schützen. Vorgänge, wie das Überprüfen, das Erstellen von Berichten und das Drucken, sind nicht durch ein Kennwort geschützt.

Gehen Sie zum Festlegen eines Kennworts folgendermaßen vor.

1. Klicken Sie zum Öffnen des Funktionsblock-Editors mit der rechten Maustaste auf einen benutzerdefinierten Funktionsblock, und wählen Sie „Edit“ (Bearbeiten) aus.

2. Wählen Sie im Funktionsblock-Editor die Option „File > Change Password“ (Datei > Kennwort ändern) aus.



3. Geben Sie im Feld „New Password“ (Neues Kennwort) ein Kennwort aus maximal sechs alphanumerischen Zeichen ein.

4. Geben Sie das Kennwort im Feld „Confirm Password“ (Kennwort bestätigen) erneut ein.

5. Klicken Sie auf „OK“.

Der benutzerdefinierte Funktionsblock kann ohne die Eingabe dieses Kennworts weder bearbeitet noch gelöscht werden.

Wir empfehlen Ihnen die Verwendung eines Kennworts zum Schutz von getesteten benutzerdefinierten Funktionsblöcken, um nicht autorisierte oder unbeabsichtigte Änderungen zu verhindern, nachdem der Funktionsblock in einem Anwenderprogramm zugeordnet wurde.

Wiederverwenden der Dateien mit benutzerdefinierten Funktionsblöcken

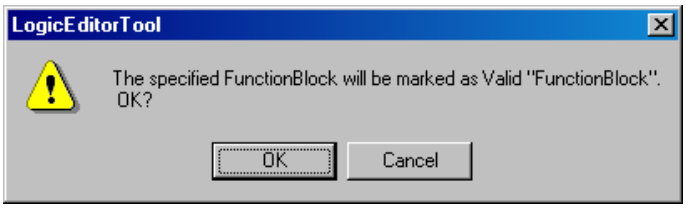
Projektdateien (*.dnt) und Dateien mit benutzerdefinierten Funktionsblöcken (*.fbd) sind voneinander getrennt. Sie können die Dateien mit benutzerdefinierten Funktionsblöcken beim Erstellen von Programmen wiederverwenden. Für das Importieren, Speichern, Löschen, Überprüfen und Bearbeiten von benutzerdefinierten Funktionsblöcken benötigen Sie Windows-Administratorrechte.

Gehen Sie zum Wiederverwenden benutzerdefinierter Funktionsblöcke folgendermaßen vor.

1. Erstellen Sie den benutzerdefinierten Funktionsblock wie auf Seite 158 beschrieben.

2. Überprüfen Sie die Ausführung des benutzerdefinierten Funktionsblocks.
   a. Klicken Sie in der Objektliste im Logik-Editor mit der rechten Maustaste auf den neuen Funktionsblock, und wählen Sie „Edit“ (Bearbeiten) aus.
   b. Überprüfen Sie das Funktionsblockprogramm, und beheben Sie mögliche Probleme.
   c. Sofern Sie Änderungen vorgenommen haben, speichern Sie das Funktionsblockprogramm.
   d. Schließen Sie den Funktionsblocklogik-Editor.

3. Überprüfen Sie den benutzerdefinierten Funktionsblock.
   a. Klicken Sie in der Objektliste im Logik-Editor mit der rechten Maustaste auf den neuen Funktionsblock, und wählen Sie „Validate“ (Überprüfen) aus.
   b. Klicken Sie im Bestätigungsdialogfeld auf „OK“.

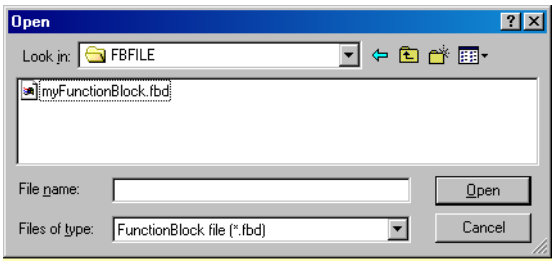
   

   Das Symbol für den neuen Funktionsblocks wechselt von Weiß zu Gelb und gibt dadurch an, dass der Funktionsblock überprüft wurde.

4. Exportieren Sie den benutzerdefinierten Funktionsblock in eine Datei.
   a. Klicken Sie in der Objektliste im Logik-Editor auf den gespeicherten benutzerdefinierten Funktionsblock.
   b. Wählen Sie im Hauptmenü „FunctionBlock > Export“ (Funktionsblock > Exportieren) aus.
   c. Geben Sie im Dialogfeld „Save As“ (Speichern unter) einen Namen für die Datei ein und klicken Sie auf „Save“ (Speichern).

5. Verschieben oder kopieren Sie die Datei ggf. auf andere PCs.

6. Importieren Sie den benutzerdefinierten Funktionsblock.
   a. Erstellen Sie in RSNetWorx for DeviceNet ein neues Projekt, und fügen Sie eine SmartGuard-Steuerung hinzu.
   b. Klicken Sie mit der rechten Maustaste auf die Steuerung, wählen Sie „Properties“ (Eigenschaften) und anschließend die Registerkarte „Logic“ (Logik) aus.
   c. Klicken Sie auf „Edit“ (Bearbeiten), um den Logik-Editor zu starten.
   d. Wählen Sie „FunctionBlock > Import“ (Funktionsblock > Importieren) aus.



   e. Wählen Sie die entsprechende Datei aus, und klicken Sie auf „Open“ (Öffnen).

      Der importierte benutzerdefinierte Funktionsblock wird in der Objektliste im Logik-Editor angezeigt.

WICHTIG Sie sollten immer zunächst die Dateien mit benutzerdefinierten Funktionsblöcken importieren, bevor Sie Anwendungsprogramme bearbeiten oder überprüfen, in denen diese Dateien verwendet werden.

Hinweise für das Wiederverwenden von benutzerdefinierten Funktionsblöcken

In der folgenden Tabelle wird angegeben, für welche Aktionen die Dateien mit benutzerdefinierten Funktionsblöcken erforderlich sind und was passiert, wenn die Aktion ausgeführt wird, ohne dass die Funktionsblockdatei verfügbar ist.

Ergebnis ohne Funktionsblockdateien

Aktion	Datei	Ergebnis
Herunterladen	Nicht erforderlich	Normale Ausführung
Hochladen	Nicht erforderlich	Normale Ausführung
Speichern der Projektdatei	Nicht erforderlich	Normale Ausführung
Laden der Projektdatei	Nicht erforderlich	Normale Ausführung

Ergebnis ohne Funktionsblockdateien

Aktion	Datei	Ergebnis
Überprüfung	Erforderlich	Die Programmüberprüfung kann auch ohne die Funktionsblockdatei abgeschlossen werden, wenn die Datei bereits auf die Steuerung heruntergeladen wurde. Dabei kann jedoch nicht die Konfiguration des Funktionsblocks überprüft werden.
Bearbeiten des Programms	Erforderlich	Es wird eine Warnung angezeigt, wenn der Logik-Editor ohne die Funktionsblockdatei geöffnet wird. Der benutzerdefinierte Funktionsblock ohne Datei wird mit einem -Symbol angezeigt, und sämtliche Verbindungen zu und von dem Funktionsblock werden gelöscht. Bearbeitungsfunktionen wie Kopieren und Einfügen sind nicht verfügbar. Wenn das Programm geändert wird, kann es weder gespeichert noch heruntergeladen werden.
Anwenden des Programms	Erforderlich	Dieser Befehl kann ohne die Datei mit dem benutzerdefinierten Funktionsblock nicht ausgeführt werden.

TIPP

Wenn Sie die Datei mit dem benutzerdefinierten Funktionsblock importieren, während das Programm geöffnet ist, wird dieses nicht automatisch aktualisiert. Schließen Sie das Programm, und öffnen Sie es erneut, um den Funktionsblock richtig anzuzeigen.

WICHTIG

Überprüfen Sie immer das Originalprogramm, nachdem Sie benutzerdefinierte Funktionsblöcke bearbeitet haben. Wenn Sie einen benutzerdefinierten Funktionsblock erstellt, im Originalprogramm verwendet und dann nach dem Speichern des Originalprogramms bearbeitet haben, wird der Funktionsblock im Programm nicht aktualisiert.

Zusätzliche Hilfsmittel

Hilfsmittel	Beschreibung
Anhang C, Befehlsreferenz zu den Logikfunktionen	Enthält detaillierte Informationen über logische Funktionen.
Anhang D, Befehlsreferenz zu den Funktionsblöcken	Enthält detaillierte Informationen über Funktionsblöcke.

Notizen:

Herunterladen und Überprüfen

Einleitung

Thema	Seite
Herunterladen der DeviceNet-Netzwerkkonfiguration	165
Überprüfen der DeviceNet-Sicherheitskonfiguration	167
Starten des Assistenten zur Überprüfung von Sicherheitsgeräten	167
Ermitteln, ob Geräte überprüft werden können	168
Auswählen der zu prüfenden Geräte	169
Überprüfen der Prüfberichte für Sicherheitsgeräte	171
Verriegeln von Sicherheitsgeräten	172
Überprüfen der Zusammenfassung des Assistenten zur Überprüfung von Sicherheitsgeräten	173

Herunterladen der DeviceNet-Netzwerkkonfiguration

Vor dem Herunterladen müssen Sie mithilfe der Software RSNetWorx for DeviceNet eine Verbindung mit dem DeviceNet-Netzwerk herstellen. Der Computer und die Geräte, mit denen Sie kommunizieren möchten, müssen mit dem DeviceNet-Netzwerk verbunden sein. Wenn Sie die Steuerung hingegen im eigenständigen Modus ausführen, muss der Computer mit dem USB-Anschluss der SmartGuard-Steuerung verbunden sein.

Wenn Sie über das EtherNet/IP-Protokoll mit der SmartGuard-Steuerung verbunden sind, müssen Sie wie in diesem Abschnitt beschrieben vorgehen. Wenn Sie eine Verbindung mit der SmartGuard-Steuerung über das EtherNet/IP-Protokoll hergestellt haben, wird im Grunde genommen eine Überbrückung durch die SmartGuard-Steuerung zum DeviceNet-Netzwerk vorgenommen und in den Online-Modus gewechselt, damit Sie die Funktionen zum Herunterladen und Überwachen ausführen können. Zwar konzentriert sich dieses Kapitel auf die Verwendung des DeviceNet-Protokolls, doch gelten dieselben Anweisungen auch für das EtherNet/IP-Protokoll.

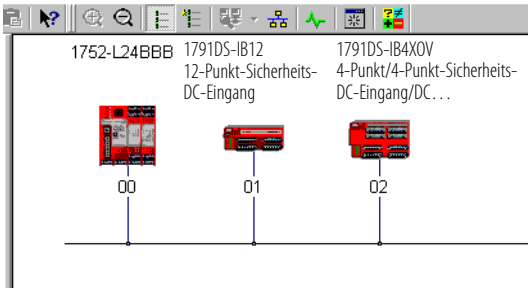
Wenn Sie eine Online-Verbindung mit einem DeviceNet-Netzwerk herstellen, durchsucht die Software RSNetWorx for DeviceNet das Netzwerk einmal und zeigt die Geräte im Netzwerk an. Dabei werden die Parameter der Geräte weder gelesen (hochladen) noch geändert (herunterladen).

Die bei dem Suchvorgang erstellte grafische Darstellung des Netzwerks bleibt statisch. Sie wird nur dann automatisch aktualisiert, um Änderungen seit dem letzten Suchvorgang anzuzeigen, wenn die Option „Continuous Browse“ (Kontinuierliches Durchsuchen) aktiviert wurde.

Gehen Sie zum Herunterladen der DeviceNet-Netzwerkkonfiguration folgendermaßen vor.

1. Stellen Sie eine Online-Verbindung her, indem Sie auf das Symbol Online klicken.

2. Wechseln Sie zum DeviceNet-Netzwerk, und klicken Sie bei der Aufforderung auf „OK“.



Bei jedem Suchvorgang liest RSNetWorx for DeviceNet die folgenden Attribute der einzelnen Geräte.

Sicherheitsattribut	Beschreibung
Kombination aus Sicherheitsnetzwerknummer (SNN) und Netzknotenadresse	Die in der RSNetWorx for DeviceNet-Konfigurationsdatei gespeicherte Netzwerknotenadresse und SNN müssen mit der Netzknotenadresse und SNN des Online-Geräts übereinstimmen. Wenn die SNNs nicht übereinstimmen, wird für das Gerät der SNN-Fehlerstatus angezeigt. Weitere Informationen zum Beheben nicht übereinstimmender SNNs finden Sie auf Seite 67.
Konfigurationssignatur	RSNetWorx for DeviceNet vergleicht die Konfigurationssignatur in der Konfigurationsdatei mit der Konfigurationssignatur im Online-Gerät.
Sicherheitsverriegelung	Wenn das Gerät über eine Sicherheitsverriegelung verfügt, kann seine Konfiguration erst nach dem Freigeben des Geräts geändert werden.

3. Laden Sie die Konfiguration auf das Netzwerk herunter, indem Sie mit der rechten Maustaste auf das Gerät klicken und dann „Download to Device“ (Auf Gerät herunterladen) auswählen.

4. Bestätigen Sie die Download-Absicht, indem Sie auf „Yes“ (Ja) klicken.

   Wenn ein Gerät kennwortgeschützt ist, fordert Sie RSNetWorx for DeviceNet zur Eingabe des Kennworts für die einzelnen geschützten Geräte auf.

   Wenn ein Gerät über eine Sicherheitsverriegelung verfügt, müssen Sie es zunächst freigeben, bevor Sie den Download-Vorgang starten.

WICHTIG Wenn Sie die Sicherheitsverriegelung eines Geräts aufheben, müssen Sie den Assistenten zur Überprüfung von Sicherheitsgeräten ausführen, um das Gerät vor dem Betrieb im Sicherheitssystem erneut zu überprüfen und die Sicherheitsverriegelung wieder zu aktivieren.

TIPP

Wenn keines der Geräte über einen Kennwortschutz oder eine Sicherheitsverriegelung verfügt, können Sie im Menü „Network" (Netzwerk) die Option „Download to Network" (Ins Netzwerk herunterladen) auswählen, um die Konfiguration in das Netzwerk herunterzuladen. Bei diesem Schritt werden jedoch Geräte übersprungen, die über einen Kennwortschutz oder eine Sicherheitsverriegelung verfügen.

Überprüfen der DeviceNet-Sicherheits-konfiguration

WICHTIG

Vor dem Ausführen des Assistenten zur Überprüfung von Sicherheitsgeräten sollten Sie das Netzwerk durchsuchen und hochladen und die Sicherheitsgeräte sowie deren sämtliche Sicherheitsfunktionen im Netzwerk testen, um ihre ordnungsgemäße Funktion sicherzustellen. Sie müssen die Anwendungen vollständig testen, bevor Sie die Sicherheitsverriegelung der Geräte aktivieren.

Weitere Informationen zum Überprüfen von Sicherheitsanwendungen finden Sie im Sicherheitsreferenzhandbuch für die SmartGuard-Steuerungen, Publikation 1752-RM001.

Der Assistent zur Überprüfung von Sicherheitsgeräten, den Sie in der Software RSNetWorx for DeviceNet finden, führt Sie durch die für das Überprüfen der Konfiguration des Sicherheitsgeräts erforderlichen Schritte und stellt Möglichkeiten für die Sicherheitsverriegelung dieser Geräte bereit. Die Überprüfung umfasst das Hochladen und Vergleichen der im Gerät gespeicherten Konfiguration mit der in der Konfigurationsdatei von RSNetWorx for DeviceNet gespeicherten Konfiguration. Die Konfiguration wird in einem Bericht angezeigt, der eine visuelle Überprüfung und das Protokollieren der Ergebnisse ermöglicht.

WICHTIG

Einige Geräte im Netzwerk unterstützen möglicherweise nicht die Überprüfung durch den Assistenten zur Überprüfung von Sicherheitsgeräten. In der Anwenderdokumentation finden Sie Informationen dazu, wie diese Geräte überprüft werden können.

Starten des Assistenten zur Überprüfung von Sicherheitsgeräten

Gehen Sie zum Ausführen des Assistenten zur Überprüfung von Sicherheitsgeräten folgendermaßen vor.

1. Wählen Sie „Network > Safety Device Verification Wizard" (Netzwerk > Assistent zur Überprüfung von Sicherheitsgeräten).

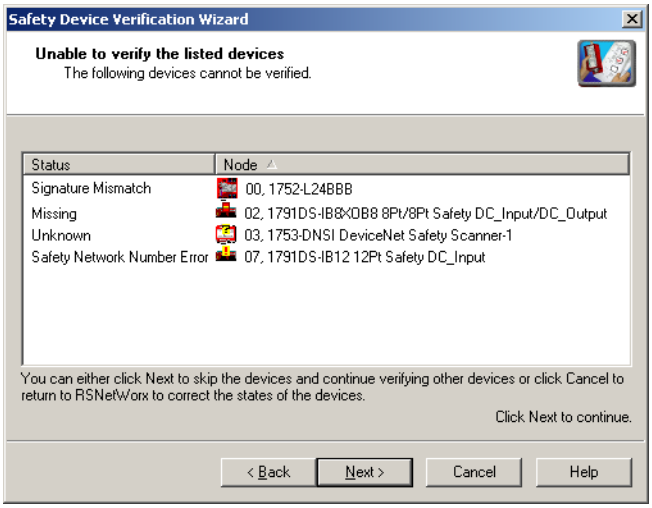
   Das Dialogfeld „Welcome" (Willkommen) wird angezeigt. Es enthält eine Beschreibung des Prüfvorgangs.

2. Klicken Sie auf „Next" (Weiter).

Ermitteln, ob Geräte überprüft werden können

Während der Assistent zur Überprüfung von Sicherheitsgeräten das Netzwerk durchsucht, prüft er den Sicherheitsstatus der Geräte im Netzwerk, um zu ermitteln, ob diese überprüft werden können.

Wenn sich Geräte in einem Status befinden, der verhindert, dass der Assistent die Überprüfung fortsetzen kann, erscheint das Dialogfeld „Unable to verify the listed devices“ (Überprüfung der aufgelisteten Geräte nicht möglich), das diese Geräte mit ihrem aktuellen Status mittels eines Gerätesymbols und eines Statussymbols anzeigt.



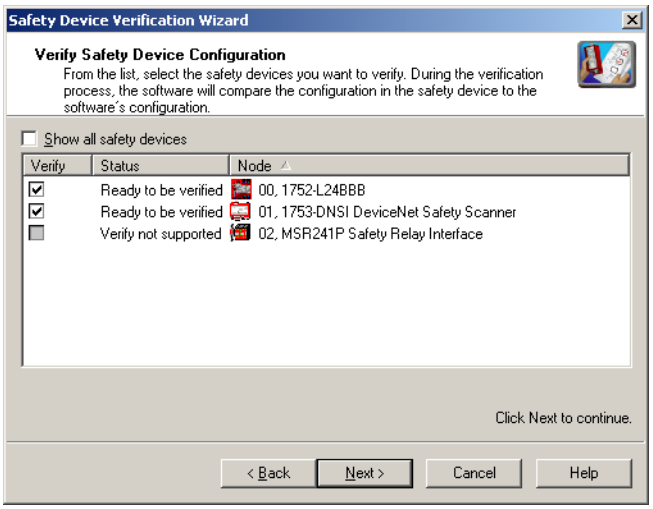
Status	Statussymbol	Beschreibung
Fehlt		Das Gerät ist Teil der Netzwerkkonfiguration, wurde jedoch beim Suchvorgang nicht gefunden.
Abweichung		Die Geräteidentität in der Netzwerkkonfiguration stimmt nicht mit der Identität des Online-Geräts überein.
Unbekannt		Das Gerät ist in der Konfiguration enthalten, wurde jedoch im Netzwerk noch nicht gefunden.
Fehler bei der Sicherheitsnetz-werknummer		Die Sicherheitsnetzwerknummer (SNN) im Gerät ist entweder ungültig oder stimmt nicht mit der SNN für das Gerät in der Konfigurationsdatei von RSNetWorx for DeviceNet überein.
Signaturab-weichung	Kein	Die Konfigurationssignatur des Geräts stimmt nicht mit der Konfigurationssignatur in der Konfigurationsdatei von RSNetWorx for DeviceNet überein.
Sicherheitsver-riegelung		Die Sicherheitsverriegelung für das Gerät wurde bereits aktiviert.

Um den Status der angegebenen Geräte korrigieren zu können, müssen Sie zurück zu RSNetWorx for DeviceNet wechseln. Schließen Sie dafür den Assistenten zur Überprüfung von Sicherheitsgeräten, indem Sie auf „Cancel“ (Abbrechen) klicken.

Wenn Sie die aufgeführten Geräte überspringen und mit der Überprüfung anderer Sicherheitsgeräte im Netzwerk fortfahren möchten, klicken Sie auf „Next“ (Weiter).

Auswählen der zu prüfenden Geräte

Sie wählen die zu überprüfenden Geräte mithilfe der Kontrollkästchen in der Spalte „Verify“ (Überprüfen) im Dialogfeld „Verify Safety Device Configuration“ (Konfiguration der Sicherheitsgeräte überprüfen) aus. Sie können nur solche Geräte auswählen, deren Status „Ready to be verified“ (Bereit zur Überprüfung) ist.



Wenn das Kontrollkästchen „Show all safety devices“ (Alle Sicherheitsgeräte zeigen) aktiviert ist, werden im Dialogfeld sämtliche Sicherheitsgeräte im Netzwerk mit ihrem aktuellen Status aufgeführt. Wenn das Kontrollkästchen deaktiviert ist (Standardeinstellung), werden nur Geräte mit folgendem Status angezeigt:

- Verify FAILED (Überprüfung fehlgeschlagen)

  Beim Hochladen und Vergleichen wurde festgestellt, dass die Konfiguration im Gerät nicht mit der in der Konfigurationsdatei von RSNetWorx for DeviceNet übereinstimmt.

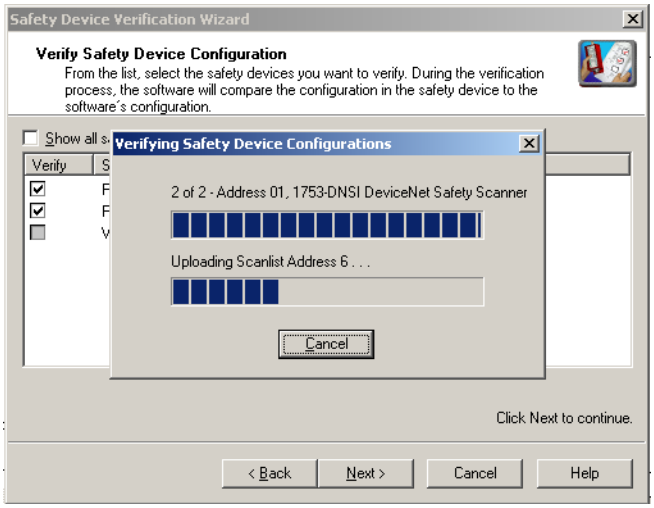
- Ready to be verified (Bereit zur Überprüfung)

  Das Gerät verfügt über keine Sicherheitsverriegelung und kann für die Überprüfung ausgewählt werden.

- Verify not supported (Überprüfung nicht unterstützt)

  Das Gerät verfügt nicht über eine Sicherheitsverriegelung, unterstützt jedoch nicht die Überprüfung mit dem Assistenten zur Überprüfung von Sicherheitsgeräten. Weitere Informationen zum Überprüfen dieses Geräts finden Sie in der Anwenderdokumentation. Nachdem das Gerät überprüft wurde, kann der Assistent für dieses die Sicherheitsverriegelung aktivieren.

Klicken Sie auf „Next“ (Weiter), um das Hochladen und Vergleichen zu starten.



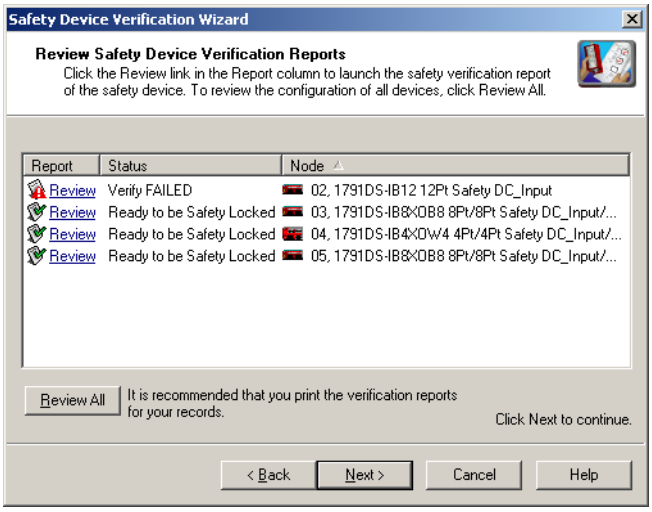
TIPP

Wenn Sie auf„Next“ (Weiter) klicken, ohne ein zu überprüfendes Gerät auszuwählen, prüft der Assistent, ob bei dieser Ausführung des Assistenten Geräte überprüft wurden oder ob die Sicherheitsverriegelung für diese Geräte aktiviert werden kann.

Wenn	Anzeige im Assistenten
Diese Geräte wurden überprüft	Im Dialogfeld„Review“ (Überprüfen) werden diese Geräte aufgeführt.
Die Sicherheitsverriegelung kann für diese Geräte aktiviert werden.	Im Dialogfeld„Lock“ (Verriegeln) werden diese Geräte aufgeführt.
Es wurden keine Geräte überprüft.	Das Dialogfeld„Finish“ (Fertig stellen) wird angezeigt.
Die Sicherheitsverriegelung kann für keine Geräte aktiviert werden	Das Dialogfeld„Finish“ (Fertig stellen) wird angezeigt.

Überprüfen der Prüfberichte für Sicherheitsgeräte

Auf der Seite „Review“ (Überprüfen) werden die Sicherheitsgeräte mit dem Status „Verify FAILED“ (Überprüfung fehlgeschlagen) oder „Ready to be Safety Locked“ (Bereit zur Sicherheitsverriegelung) angezeigt.



1. Klicken Sie in der Spalte „Report“ (Bericht) auf „Review“ (Überprüfen), um den HTML-Bericht des Geräts im Standardbrowser anzuzeigen.
2. Klicken Sie auf „Review All“ (Alle überprüfen), um einen HTML-Prüfbericht über sämtliche aufgeführten Geräte zu erhalten.

   TIPP Wenn der Status eines Geräts „Verify FAILED“ (Überprüfung fehlgeschlagen) lautet, finden Sie im Prüfbericht weitere Informationen zum Fehler.

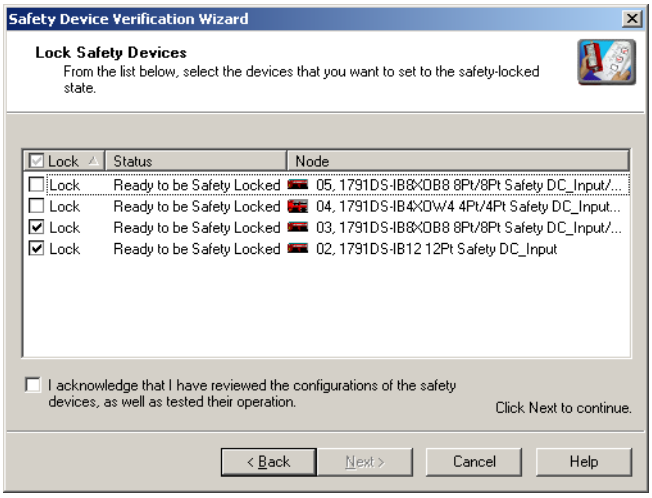
3. Sichten Sie die Prüfberichte, und drucken Sie sie für Ihre Unterlagen aus.

WICHTIG Sie müssen die Gerätekonfigurationen überprüfen und die Konfigurationssignaturen vor der Ausführung einer Sicherheitsanwendung aufzeichnen.

Verriegeln von Sicherheitsgeräten

WICHTIG Bevor Sie Sicherheitsgerätekonfigurationen verriegeln, müssen Sie sämtliche für die Anwendung erforderlichen Überprüfungen durchführen.

1. Wählen Sie die einzelnen Geräte, die zur Sicherheitsverriegelung bereit sind, durch Aktivieren der Kontrollkästchen in der Spalte „Lock“ (Verriegeln) aus.



2. Sie müssen das Bestätigungskontrollkästchen aktivieren, bevor der Verriegelungsvorgang fortgesetzt werden kann.

3. Klicken Sie auf „Next“ (Weiter).

   Der Assistent führt einen letzten Vergleich der Konfigurationssignatur in den einzelnen Sicherheitsgeräten mit der Konfigurationssignatur in RSNetWorx for DeviceNet durch, bevor die Sicherheitsverriegelung für die Geräte aktiviert wird.

4. Wenn für bestimmte Geräte ein Kennwortschutz aktiviert wurde, werden Sie zur Eingabe des Kennworts für das Gerät aufgefordert.

   Wenn Sie das Gerät auslassen möchten und die Verriegelung für die anderen Geräte fortsetzen möchten, klicken Sie auf „Skip“ (Überspringen).

Überprüfen der Zusammenfassung des Assistenten zur Überprüfung von Sicherheitsgeräten

Vor dem Beenden des Assistenten wird eine Zusammenfassung aller Sicherheitsgeräte angezeigt, für die die Sicherheitsverriegelung aktiviert wurde, sowie die Anzahl der Sicherheitsgeräte, für die noch eine Sicherheitsverriegelung aussteht. Außerdem können Sie für sämtliche Geräte im Netzwerk, für die eine Überprüfung oder eine Sicherheitsverriegelung durchgeführt wurde, den Status anzeigen.

Klicken Sie auf „Finish“ (Fertig stellen), um den Assistenten zu schließen.

Notizen:

Zustandsüberwachung und Fehlerbehebung

Einleitung

Thema	Seite
Statusanzeigen	175
Alphanumerische Anzeige	176
Überwachen des E/A-Stromversorgungseingangs	177
Überwachen der E/A-Wartungsinformationen	178
Anzeigen von E/A-Statusdaten	181
Steuerungsanschlussstatus (Sicherheits-Slave-Funktion)	184
Fehlerkategorien	187
Tabelle mit der Fehlerhistorie	188
Meldungen der Fehlerhistorie und erforderliche Maßnahmen	191
Download-Fehler und Abhilfemaßnahmen	196
Rücksetzfehler und Abhilfemaßnahmen	198
Modusänderungsfehler und Abhilfemaßnahmen	200

Statusanzeigen

Die Steuerung SmartGuard 600 ist mit Statusanzeigen für den Status von Modulen, DeviceNet- und EtherNet/IP-Netzwerk, Verriegelung, USB- und EtherNet/IP-Kommunikation, den Status einzelner Ein- und Ausgänge sowie mit einer alphanumerischen Anzeige für DeviceNet-Fehlercodes, die DeviceNet-Netzknotenadresse und EtherNet/IP-Adressinformationen ausgestattet.

Eine Beschreibung der Farb-/Statuskombinationen der Statusanzeigen und der empfohlenen Vorgehensweisen finden Sie in Anhang B.

Alphanumerische Anzeige

Die alphanumerische Anzeige der Steuerung informiert über DeviceNet-Fehlercodes, DeviceNet-Netzknotenadresse und EtherNet/IP-Adresse. Bei normalen Betriebsbedingungen ist auf der Anzeige die Netzknotenadresse des Moduls (00 bis 63) in dezimaler Angabe zu sehen. Wenn die Steuerung in einer eigenständigen Konfiguration (also ohne Netzwerk) eingesetzt wird, erscheint in der Anzeige die Zeichenfolge „nd“. Während des Selbsttests, der Konfiguration und im Leerlauf-Modus der Steuerung blinkt die Anzeige. Liegt ein Fehler vor, wird abwechselnd der Fehlercode und die Adresse des Netzknotens angezeigt, bei dem der Fehler aufgetreten ist. Bei einem schweren Fehler wird nur der Fehlercode angezeigt.

Wenn der Service-Schalter gedrückt wird, zeigt die Anzeige jeweils zwei Stellen der Sicherheits-Konfigurationssignatur der Steuerung an. Die Konfigurationssignatur kann auch in der Software RSNetWorx for DeviceNet auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften) angezeigt werden. Mithilfe der Konfigurationssignatur können Sie sich vergewissern, dass das Programm und die Konfiguration der Steuerung nicht geändert wurden.

Wenn der Schalter für die Anzeige der IP-Adresse mindestens 1 Sekunde lang gedrückt wird, erscheint in der Anzeige die festgelegte EtherNet/IP-Adresse. Der Fehlercode „n4“ wird angezeigt, wenn in der EtherNet/IP-Konfiguration ein Fehler auftritt.

Erläuterung des Anzeigenbetriebs

<table>
<tr><th colspan="2">Status</th><th colspan="2">Anzeige</th></tr>
<tr><td rowspan="3">Normaler Zustand mit aktiviertem DeviceNet</td><td>Betriebsmodus: Run (Betrieb)
Sicherheits-E/A-Kommunikation: in Betrieb</td><td rowspan="3">Die Netzknotenadresse der Steuerung.</td><td>Leuchtet</td></tr>
<tr><td>Betriebsmodus: Run (Betrieb)
Sicherheits-E/A-Kommunikation: nicht in Betrieb</td><td>Blinkt</td></tr>
<tr><td>Betriebsmodus: Selbsttest, Konfiguration oder Leerlauf</td><td>Blinkt</td></tr>
<tr><td rowspan="2">Normaler Zustand mit deaktiviertem DeviceNet</td><td>Betriebsmodus: Run (Betrieb)</td><td rowspan="2">nd</td><td>Leuchtet</td></tr>
<tr><td>Betriebsmodus: Selbsttest, Konfiguration oder Leerlauf</td><td>Blinkt</td></tr>
<tr><td rowspan="3">Fehlerbedingungen</td><td>Kritischer Fehler</td><td>Nur Fehlercode</td><td>Leuchtet</td></tr>
<tr><td>Abbrechen</td><td>Nur Fehlercode</td><td>Leuchtet</td></tr>
<tr><td>Nicht kritischer Fehler</td><td colspan="2">Wechselt zwischen Fehlercode und der Adresse des Netzknotens, an dem der Fehler aufgetreten ist.</td></tr>
</table>

Eine Beschreibung der Kombinationen von Statusanzeigen und alphanumerischen Anzeigecodes, einschließlich der erforderlichen Maßnahmen, finden Sie in Anhang B.

Überwachen des E/A-Stromversorgungseingangs

Sie können den E/A-Stromversorgungseingang sowie die allgemeinen Statusdaten der DeviceNet-E/A-Kommunikation über die alphanumerische Anzeige an der Vorderseite der Steuerung überwachen.

Wenn eine E/A-Klemme der Steuerung auf etwas anderes als „Not Used“ (Nicht belegt) eingestellt ist und keine normale Versorgungsspannung anliegt, wird auf der alphanumerischen Anzeige Folgendes angezeigt:

- P4: The power supply for inputs (V1,G1) is out of range.
  (Die Stromversorgung für Eingänge (V1,G1) befindet sich außerhalb des zulässigen Bereichs.)
- P5: The power supply for outputs (V2,G2) is out of range.
  (Die Stromversorgung für Ausgänge (V2,G2) befindet sich außerhalb des zulässigen Bereichs.)

Überwachen der E/A-Wartungsinformationen

Sie können für jede zentrale Eingangs-, Testausgangs- und zentrale Ausgangsklemme einen Wartungsmodus und einen Alarmschwellenwert konfigurieren. Dies erfolgt in der Software RSNetWorx for DeviceNet auf der Registerkarte „Maintenance“ (Wartung) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften). Sie können Klemmen für die Kontaktbetriebszähler- oder die Gesamtaktivzeit-Überwachung konfigurieren.

Kontaktbetriebszähler-Überwachung

Bei dieser Wartungsfunktion wird die Zahl der Aus-zu-Ein-Übergänge an einer zentralen Eingangs-, Testausgangs- oder zentralen Ausgangsklemme gezählt und die Zahl intern im nicht flüchtigen Speicher gespeichert.

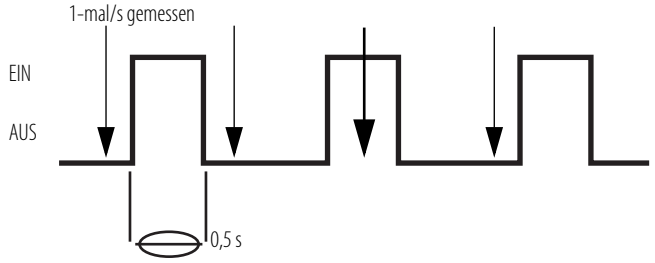
Gesamtaktivzeit-Überwachung

Bei dieser Wartungsfunktion wird gemessen, wie lang eine zentrale Eingangs-, Testausgangs- oder zentrale Ausgangsklemme den Ein-Zustand aufweist und diese Gesamtaktivzeit intern im nicht flüchtigen Speicher gespeichert. Mit der Überwachungsfunktion wird jede Sekunde geprüft, ob das angeschlossene Gerät den Ein-Zustand aufweist. Wenn das Gerät für weniger als eine Sekunde eingeschaltet ist, weist die Gesamtaktivzeit möglicherweise Abweichungen auf.

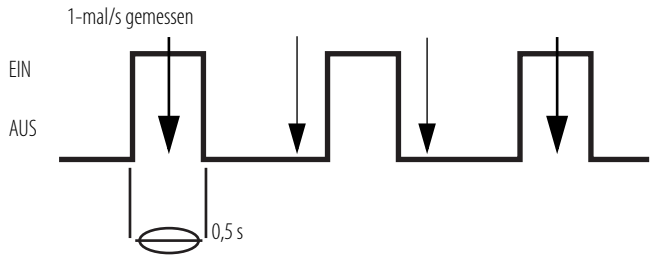
BEISPIEL

Berechnen der Gesamtaktivzeit mit Einschaltimpulsen von 0,5 s Dauer

In diesem ersten Beispiel ist das Bit für 0,5 s x 3 = 1,5 s gesetzt. Das Bit ist jedoch nur einmal beim Prüfen des Status gesetzt, sodass die Gesamtaktivzeit als 1 s gemessen wird.



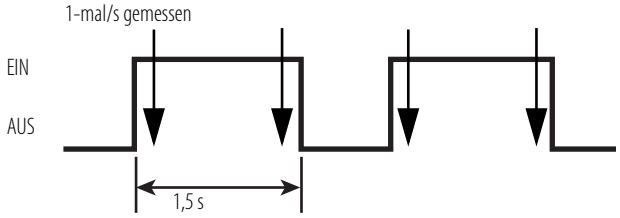
In diesem zweiten Beispiel ist das Bit für 0,5 s x 3 = 1,5 s gesetzt. Da es jedoch zweimal beim Prüfen des Status gesetzt ist, wird die Gesamtaktivzeit als 2 s gemessen.



BEISPIEL

Berechnen der Gesamtaktivzeit mit Einschaltimpulsen von 1,5 s Dauer

In diesem Beispiel ist das Bit für 1,5 s x 2 = 3 s gesetzt. Da es jedoch viermal beim Prüfen des Status gesetzt ist, wird die Gesamtaktivzeit als 4 s gemessen.

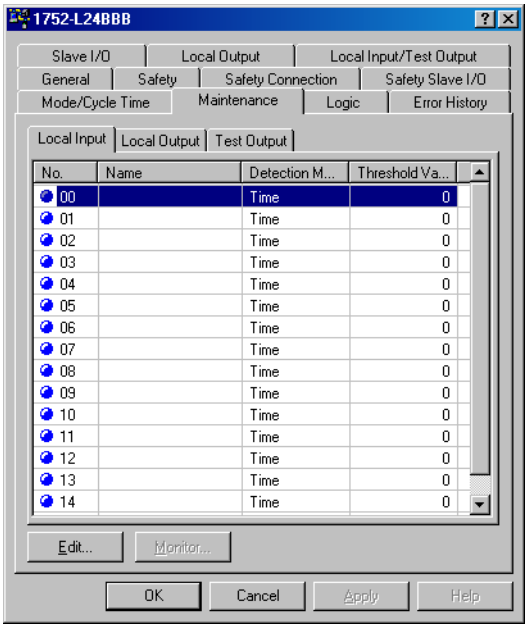


Konfigurieren eines Wartungsüberwachungsmodus

Gehen Sie folgendermaßen vor, um den Kontaktbetriebszählermodus für eine Klemme zu konfigurieren.

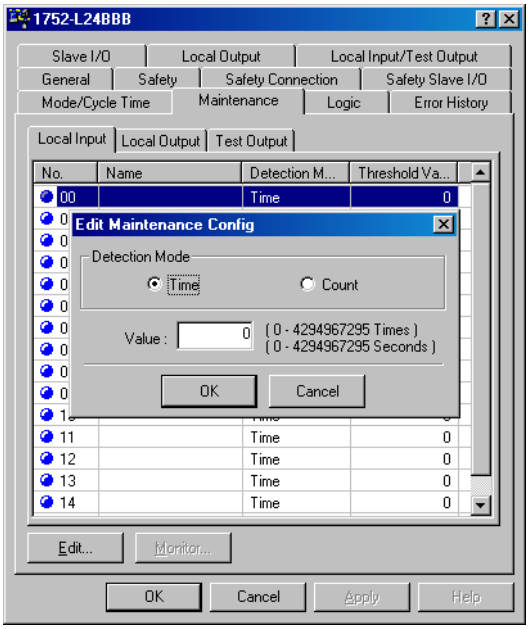
1. Klicken Sie in RSNetWorx for DeviceNet mit der rechten Maustaste auf die Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

2. Wählen Sie die Registerkarte „Maintenance“ (Wartung) aus.



3. Wählen Sie eine der Registerkarten „Local Input“ (Zentraler Eingang), „Local Output“ (Zentraler Ausgang) oder „Test Output“ (Testausgang) aus.

4. Wählen Sie die gewünschte Klemme aus, und klicken Sie auf „Edit“ (Bearbeiten).



5. Wählen Sie im Dialogfeld „Edit Maintenance Config“ (Wartungskonfiguration bearbeiten) den Erkennungsmodus aus, „Count“ (Zählen) oder „Time“ (Zeit messen).

6. Geben Sie einen Alarmschwellenwert für den gewählten Erkennungsmodus ein.

Erkennungsmodus	Gültiger Wertebereich
Zeit messen	0 bis 4 294 967 295 Sekunden
Zählen	0- bis 4 294 967 295-mal

7. Klicken Sie auf „OK“.

8. Klicken Sie auf „OK“.

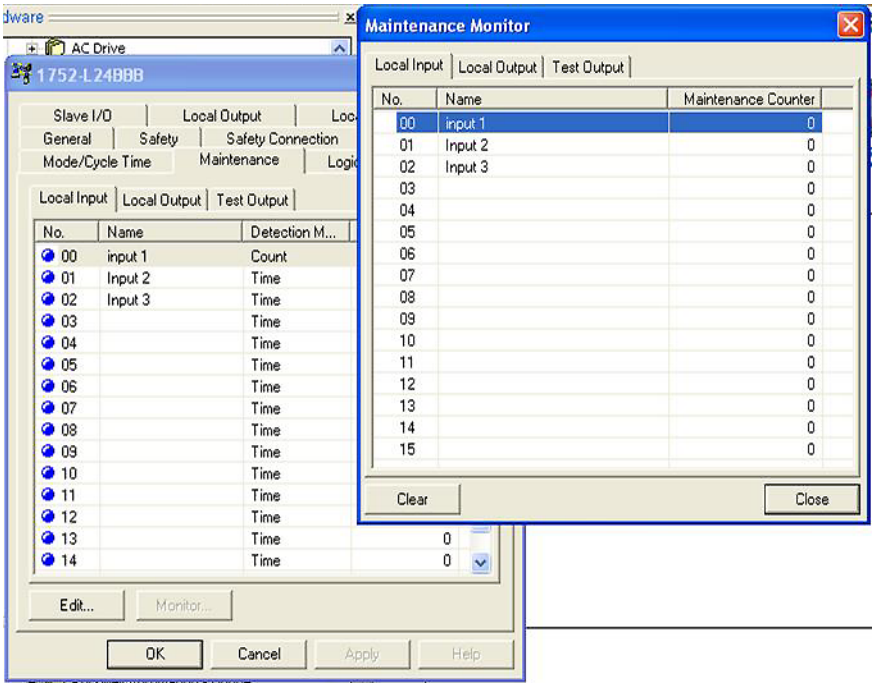
Wenn Sie mit der Steuerung online sind, können Sie die konfigurierten Klemmen überwachen, indem Sie auf der Registerkarte „Maintenance“ (Wartung) auf „Monitor“ (Überwachen) klicken.

Löschen der Wartungswerte

Gehen Sie folgendermaßen vor, um die bisherigen Zähl- oder Zeitmessungswerte zu löschen, während Sie mit der Steuerung online sind.

1. Klicken Sie auf der Registerkarte „Maintenance“ (Wartung) auf „Monitor“ (Überwachen).

2. Klicken Sie im Dialogfeld „Maintenance Monitor“ (Wartungsüberwachung) auf „Clear“ (Löschen).



Anzeigen von E/A-Statusdaten

Wenn die Steuerung als Sicherheits-Slave- oder als Standard-Slave-Ziel betrieben wird, können der ersten Zeile der übertragenen Daten Statusinformationen hinzugefügt werden. Die Informationen können in einer Steuerung gespeichert und zum Einrichten eines Überwachungssystems verwendet werden.

Steuerungsstatusdaten

Tag-Name	Datengröße	Attributtyp
Allgemeiner Status	1 Byte	Standard
Status zentraler Eingang	Wort	Sicherheit
Status zentraler Ausgang	Byte	Sicherheit
Status Testausgang/Muting-Lampe	Byte	Standard

ACHTUNG

Konfigurieren Sie das Sicherheitssteuerungssystem nicht mit Daten ohne Sicherheitsattribut. Die erforderlichen Maßnahmen für Sicherheitsdaten werden bei der Erstellung von Standarddaten nicht durchgeführt.

Allgemeine Statusdaten

Die allgemeinen Status-Flags sind Standardattribute, die den Systemstatus anzeigen.

Details zu allgemeinen Statusdaten

Bit	Name	Beschreibung
0	Status-Flag für Eingangsversorgungsspannung	Zeigt den Status der Versorgungsspannung für Eingänge an. AUS: Normale Stromversorgung ist eingeschaltet. EIN: Fehler bei der Spannungsversorgung oder Stromversorgung ist ausgeschaltet.
1	Status-Flag für Ausgangsversorgungsspannung	Zeigt den Status der Versorgungsspannung für Ausgänge an. AUS: Normale Stromversorgung ist eingeschaltet. EIN: Fehler bei der Spannungsversorgung oder Stromversorgung ist ausgeschaltet.
2	Flag für Standard-E/A-Kommunikationsfehler	Zeigt an, ob bei der Standard-E/A-Kommunikation ein Fehler vorliegt. AUS: Kein Fehler. EIN: Bei mindestens einer Standardverbindung wurde ein Fehler erkannt.
3	Flag für Standard-E/A-Kommunikationsstatus	Zeigt an, ob Standard-E/A-Kommunikation erfolgt. Das Flag ist EIN, wenn für alle Standardverbindungen normale Kommunikation erfolgt.
4	Flag für Sicherheits-E/A-Kommunikationsfehler	Zeigt an, ob bei der Sicherheits-E/A-Kommunikation ein Fehler vorliegt. AUS: Kein Fehler. EIN: Bei mindestens einer Sicherheitsverbindung wurde ein Fehler erkannt.
5	Flag für Sicherheits-E/A-Kommunikationsstatus	Zeigt an, ob Sicherheits-E/A-Kommunikation erfolgt. Das Flag ist EIN, wenn für alle Sicherheitsverbindungen normale Kommunikation erfolgt.
6	Betriebsmodus-Flag	Zeigt den Betriebsmodus der Steuerung an. AUS: Die Steuerung befindet sich nicht im Run-Modus. EIN: Die Steuerung befindet sich im Run-Modus.
7	Steuerungsstatus-Flag	Zeigt den Status der Steuerung an. AUS: Ein Fehler liegt vor. EIN: Die Steuerung wird normal betrieben.

Status zentraler Eingang

Wenn das Bit EIN ist, liegt ein normaler Status des Eingangs vor. Wenn das Bit AUS ist, wurde ein Fehler erkannt.

Klemmenstatus zentraler Sicherheitseingang

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemme 7	Klemme 6	Klemme 5	Klemme 4	Klemme 3	Klemme 2	Klemme 1	Klemme 0
1	Klemme 15	Klemme 14	Klemme 13	Klemme 12	Klemme 11	Klemme 10	Klemme 9	Klemme 8

Status zentraler Ausgang

Wenn das Bit EIN ist, liegt ein normaler Status des Ausgangs vor. Wenn das Bit AUS ist, wurde ein Fehler erkannt.

Klemmenstatus zentraler Sicherheitsausgang

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Klemme 7	Klemme 6	Klemme 5	Klemme 4	Klemme 3	Klemme 2	Klemme 1	Klemme 0

Status Testausgang oder Muting-Lampe

Wenn das Bit EIN ist, liegt ein normaler Status des Testausgangs vor. Wenn das Bit AUS ist, wurde ein Fehler erkannt.

Status Testausgang/Muting-Lampe

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Trennung von Klemme 3 erkannt	Reserviert			Klemme 3	Klemme 2	Klemme 1	Klemme 0

Steuerungsanschlussstatus (Sicherheits-Slave-Funktion)

Code	Status	Erforderliche Maßnahmen
00:0001	Normale Kommunikation	Der Status der Sicherheits-E/A-Verbindung ist normal.
01:0001	Timeout der Sicherheits-E/A-Verbindung	Bei der Sicherheits-E/A-Verbindung ist ein Timeout aufgetreten. Überprüfen Sie Folgendes: • Weisen alle Netzknoten dieselbe Baudrate auf? • Wurde die richtige Kabellänge gewählt? • Ist die Verbindung des Kabels getrennt, oder liegt das Kabel locker? • Weisen nur beide Enden der Hauptleitung Abschlusswiderstände auf? • Liegen starke Störungen vor?
01:0106	Fehler bei Ausgangsverbindungseigentümer	Der Sicherheits-Slave hat eine Ausgangs-Sicherheits-E/A-Verbindung zu einem Safety-Master hergestellt, der beim letzten Mal eine andere Netzknotenadresse hatte.
01:0109	Datengrößenfehler	Die eingestellte Sicherheits-Slave-E/A-Größe für den Sicherheits-Slave der SmartGuard-Steuerung stimmt nicht mit der für die Sicherheits-Master-Verbindung eingestellten Größe überein. Die Sicherheits-Slave-E/A-Einstellung wurde möglicherweise geändert. Löschen Sie daher die beim Sicherheits-Master registrierten Verbindungen, und konfigurieren Sie sie erneut.
01:0110	Nicht konfiguriertes Gerät	Der Sicherheits-Slave wurde nicht konfiguriert. Laden Sie die Geräteparameter in den Sicherheits-Slave herunter.
01:0111	RPI-Fehler	Das für die Sicherheits-Master-Sicherheitsverbindung eingestellte RPI ist kleiner als die Zykluszeit des Sicherheits-Slaves.
01:0113	Fehler bei der Anzahl der Verbindungen	Die Einstellung überschreitet die maximal vom Sicherheits-Slave unterstützte Anzahl von Sicherheits-E/A-Verbindungen. Überprüfen Sie die Sicherheitsverbindungseinstellungen des entsprechenden Sicherheits-Masters.
01:0114	Fehler bei Lieferanten-ID oder Produktcode	Die Gerätedaten für das Gerät in der Konfigurationsdatei von RSNetWorx for DeviceNet stimmen nicht mit dem physischen Gerät im System überein. Stellen Sie mit dem Assistenten zur Überprüfung von Sicherheitsgeräten sicher, dass das Gerät im System mit dem in der Konfigurationsdatei übereinstimmt. Stimmen die Geräteangaben überein, konfigurieren Sie die Verbindungen zum Sicherheits-Master neu.
01:0115	Gerätetypfehler	Die Gerätedaten für das Gerät in der Konfigurationsdatei von RSNetWorx for DeviceNet stimmen nicht mit dem physischen Gerät im System überein. Stellen Sie mit dem Assistenten zur Überprüfung von Sicherheitsgeräten sicher, dass das Gerät im System mit dem in der Konfigurationsdatei übereinstimmt. Stimmen die Geräteangaben überein, konfigurieren Sie die Verbindungen zum Sicherheits-Master neu.
01:0116	Firmware-Versionsfehler	Die Gerätedaten für das Gerät in der Konfigurationsdatei von RSNetWorx for DeviceNet stimmen nicht mit dem physischen Gerät im System überein. Stellen Sie mit dem Assistenten zur Überprüfung von Sicherheitsgeräten sicher, dass das Gerät im System mit dem in der Konfigurationsdatei übereinstimmt. Stimmen die Geräteangaben überein, konfigurieren Sie die registrierten Verbindungen zum Sicherheits-Master neu.

Code	Status	Erforderliche Maßnahmen
01:0117	Verbindungspfad-fehler	Mindestens zwei Singlecast-Sicherheits-E/A-Verbindungen oder eine Multicast-Sicherheits-E/A-Verbindung mit einem anderen RPI wurden für Sicherheits-Slave-E/A eingestellt. Um Sicherheits-Slave-E/A auf einem Sicherheits-Slave mit mehr als einem Sicherheits-Master zu teilen, stellen Sie das RPI jeweils gleich ein, und legen Sie als Verbindungstyp Multicast fest. Sicherheits-Slaves von SmartGuard-Steuerungen können für alle Sicherheits-Slave-E/A nur jeweils eine Singlecast-Sicherheits-E/A-Verbindung aufweisen. Stellen Sie mehrere Verbindungspfade für die Sicherheits-Slave-E/A der Steuerung ein. Wenn das Problem durch die vorgenannten Lösungen nicht behoben werden kann, löschen Sie die Verbindungen zum Sicherheits-Master, und konfigurieren Sie sie erneut.
01:031E	Fehler bei der Anzahl der Verbindungen	Die Einstellung für die Anzahl von Sicherheits-E/A-Verbindungen überschreitet die maximal vom Sicherheits-Slave unterstützte Anzahl. Passen Sie die Sicherheitsverbindungseinstellung für den entsprechenden Sicherheits-Master an. Vergewissern Sie sich insbesondere, dass für jede Multicast-Verbindung höchstens 15 und insgesamt höchstens 60 Sicherheits-Master eingestellt sind.
01:031F	Verbindungs-ID-Ressourcenfehler	Die maximale Anzahl von Verbindungs-IDs für einen Sicherheits-Master (12) wurde überschritten. Klicken Sie im Dialogfeld „Safety Connection Properties“ (Eigenschaften der Sicherheitsverbindung) auf „Advanced“ (Erweitert). Aktivieren Sie das Kontrollkästchen „Request target device to allocate message IDs“ (Zielgerät zur Zuweisung der Meldungs-IDs anfordern). Laden Sie die Geräteparameter in den Sicherheits-Master herunter.
01:07FF	Nicht vorhandener Sicherheits-Slave	Der Sicherheits-Slave wurde möglicherweise dem Netzwerk nicht richtig hinzugefügt. Vergewissern Sie sich, dass der zugehörige Sicherheits-Slave online ist. Wenn der Sicherheits-Slave nicht online, prüfen Sie Folgendes: • Ist die Netzknotenadresse für den Sicherheits-Slave richtig? • Weisen alle Netzknoten dieselbe Kommunikationsrate auf? • Wurde die richtige Kabellänge gewählt? • Ist die Verbindung des Kabels getrennt, oder liegt das Kabel locker? • Weisen nur beide Enden der Hauptleitung Abschlusswiderstände auf? • Liegen starke Störungen vor?
01:080C	Übereinstimmung der Sicherheits-signatur	Die vom Sicherheits-Master überwachte Sicherheitssignatur für den Sicherheits-Slave stimmt nicht mit der Sicherheitssignatur des eigentlichen Sicherheits-Slaves überein. Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück, und laden Sie die Geräteparameter erneut herunter. Wenn das Problem nach diesem Vorgang immer noch besteht, löschen Sie die im Sicherheits-Master konfigurierten Verbindungen, und konfigurieren Sie sie erneut.

Code	Status	Erforderliche Maßnahmen
01:080E	Abweichung der Sicherheitsnetzwerk-nummer (SNN)	Die vom Sicherheits-Master überwachte SNN für den Sicherheits-Slave stimmt nicht mit der SNN des eigentlichen Sicherheits-Slaves überein. Setzen Sie den Sicherheits-Slave auf die Standardeinstellungen zurück, und laden Sie die richtigen Geräteparameter herunter. Wenn das Problem nach diesem Vorgang immer noch besteht, löschen Sie die im Sicherheits-Master konfigurierten Verbindungen, und konfigurieren Sie sie erneut.
D0:0001	Leerlauf-Modus	Der Sicherheits-Master der SmartGuard-Steuerung befindet sich im Leerlauf-Modus, und es wurden keine Sicherheits-E/A-Verbindungen hergestellt. Wechseln Sie den Betriebmodus der SmartGuard-Steuerung in den Ausführungsmodus (Execute).

Fehlerkategorien

Steuerungsfehler können in drei Kategorien unterteilt werden: nicht kritische Fehler, Abbruchfehler und kritische Fehler.

Steuerungsfehlerkategorien

Fehlerkategorie	Beschreibung
Nicht kritische Fehler	Ein Fehler, durch den alle zentralen oder Sicherheits-E/A-Verbindungsklemmen unterbrochen und in den Sicherheitszustand überführt werden. Die Steuerung wird weiterhin im Betriebsmodus (Run) betrieben.
Abbruchfehler	Die Steuerung verlässt den Run-Modus, wechselt in den Leerlauf-Modus und setzt alle Sicherheits-E/A in ihren Sicherheitszustand. Explizite Nachrichtenübertragungen oder teilweise Funktionen von RSNetWorx for DeviceNet werden zum Überprüfen des Fehlerstatus unterstützt.
Kritischer Fehler	Wenn ein Fehler dieses Typs auftritt, stellt die Steuerung die Funktion vollständig ein. Informationen zu Fehlern beim Herunterladen finden Sie auf Seite 196. Informationen zu Reset-Fehlern finden Sie unter Rücksetzfehler und Abhilfemaßnahmen. Informationen zu Fehlern, die beim Moduswechsel auftreten können, finden Sie unter Modusänderungsfehler und Abhilfemaßnahmen.

Tabelle mit der Fehlerhistorie

Beim Auftreten eines Fehlers wird in der Tabelle mit der Fehlerhistorie im RAM der Steuerung ein Datensatz erstellt. Überschreitet die Anzahl der Fehler das Maximum von 100, werden die ältesten Datensätze nacheinander gelöscht und die aktuellen Fehlerdaten als neuer Datensatz gespeichert.

In der Tabelle mit der Fehlerhistorie werden der Status der Steuerung beim Auftreten des Fehlers, der Zeitpunkt, zu dem der Fehler aufgetreten ist (Gesamtbetriebszeit der Steuerung[(1)]) und die Adresse des Netzknotens, an dem der Fehler aufgetreten ist, gespeichert.

Speicherbereich für die Fehlerhistorie

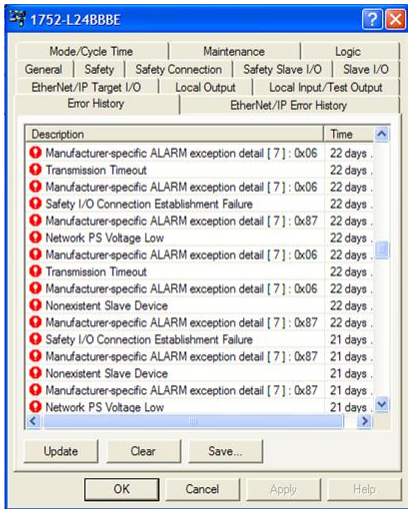
Die Beschreibung eines Fehlers wird als Fehlerhistoriendatensatz im RAM der Steuerung aufgezeichnet. Handelt es sich um einen kritischen Fehler, wird er auch im nicht flüchtigen Speicher aufgezeichnet. Die im nicht flüchtigen Speicher aufgezeichnete Fehlerhistorie wird auch beibehalten, wenn die Steuerung nicht mit Strom versorgt oder neu gestartet wird. Beim Aus- und Einschalten der Steuerung wird die Fehlerhistorie im nicht flüchtigen Speicher in den RAM der Steuerung kopiert. Die Fehlerhistorie im RAM wird beim Lesen der Fehlerhistorie aus der Software RSNetWorx for DeviceNet gelesen. Beim Löschen der Fehlerhistorie wird jedoch sowohl die Fehlerhistorie im RAM als auch die im nicht flüchtigen Speicher gelöscht.

Anzeigen der Tabelle mit der Fehlerhistorie für die Steuerung 1752-L24BBB

Gehen Sie folgendermaßen vor, um die Fehlerhistorie in Echtzeit mit RSNetWorx for DeviceNet anzuzeigen, während die Steuerung online ist.

1. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

2. Klicken Sie auf die Registerkarte „Error History“ (Fehlerhistorie).



(1) Die Gesamtbetriebszeit der Steuerung wird als verstrichene Zeit in Sprüngen von 6 Minuten bei eingeschalteter Stromversorgung für V0, G0 aufgezeichnet. Die Gesamtbetriebszeit wird durch den Reset-Befehl der Steuerung gelöscht.

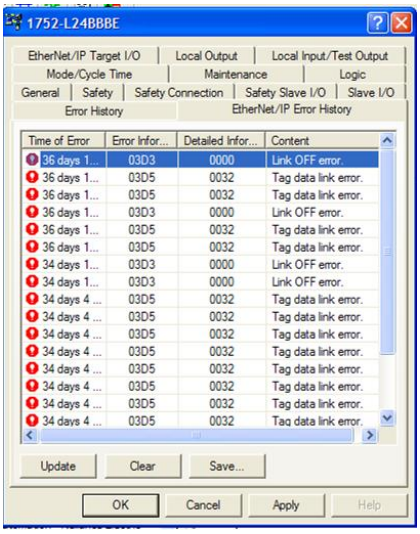
a. Klicken Sie auf „Save“ (Speichern), um die Daten der Fehlerhistorie zu speichern. Diese können auch in einer separaten CSV-Datei gespeichert werden.
b. Klicken Sie auf „Clear“ (Löschen), um die in der Steuerung gespeicherte Fehlerhistorie zu löschen.
c. Klicken Sie auf „Update“ (Aktualisieren), um die Informationen der Fehlerhistorie zu aktualisieren.

Anzeigen der Tabelle mit der EtherNet/IP-Fehlerhistorie für die Steuerung 1752-L24BBBE

Gehen Sie folgendermaßen vor, um die Fehlerhistorie in Echtzeit mit RSNetWorx for DeviceNet anzuzeigen, während die Steuerung online ist.

1. Klicken Sie mit der rechten Maustaste auf die SmartGuard-Steuerung, und wählen Sie „Properties“ (Eigenschaften) aus.

2. Klicken Sie auf die Registerkarte „EtherNet/IP Error History“ (EtherNet/IP-Fehlerhistorie).



a. Klicken Sie auf „Save“ (Speichern), um die Daten der Fehlerhistorie zu speichern. Diese können auch in einer separaten CSV-Datei gespeichert werden.
b. Klicken Sie auf „Clear“ (Löschen), um die in der Steuerung gespeicherte Fehlerhistorie zu löschen.
c. Klicken Sie auf „Update“ (Aktualisieren), um die Informationen der Fehlerhistorie zu aktualisieren.

Tabelle mit Ethernet-Fehlerhistorie

Fehlercode	Fehler	Detailcode		7-Segment-Anzeige
		1. Byte[1]	2. Byte[1]	
0602	Speicher der CPU-Buseinheit	01: Lesefehler	Variable	E9<->n4
		02; Schreibfehler		
020F	Kommunikationssteuerung	00	01	F4<->n4
0211	Doppelte IP-Adresse	02	Niederwertiges Byte der IP-Adresse	F0<->n4
021A	Logikfehler in Einstellungstabelle	00	Variable	UF
03C4	Serververbindung	04;BOOTP	01; Bestimmter Host existiert nicht	E3<0>n4
			07: Übertragungsfehler	
			08: Empfangsfehler	
			0A: Fehler beim Abrufen der IP-Adresse	
03D0	Ethernet-Basiseinstellung	01: Fehler in der Ethernet-Einstellung	01: Prüfsummenfehler	F2<->n4
			11: Inkonsistente Einstellung	
			12; Angegebene Baudrate wird nicht unterstützt	
		02: Fehler in der TCP/IP-Basiseinstellung	01: Prüfsummenfehler	
			11: Ungültige IP-Adresse	
			12: Ungültige Subnet-Maske	
			13: Ungültige Standard-Gateway-Adresse	
			14: Ungültiger primärer Namensserver	
			15: Ungültiger sekundärer Namensserver	
			16: Ungültiger Domänenserver	
			17: Ungültiger Hostname	
03D5	Tag-Datenverbund	00	Niederwertiges Byte der IP-Adresse	L9<->n4
03D3	Verbindung AUS	00	00	E1<->n4

(1) Das erste Byte wird kombiniert mit dem zweiten Byte als einzelnes 4-Hex-Zeichen in der Spalte „Detailed Information" (Detaillierte Informationen) auf der Registerkarte „EtherNet/IP Error History" (EtherNet/IP-Fehlerhistorie) angezeigt. Beispiele finden Sie im Dialogfeld, das im Abschnitt Anzeigen der Tabelle mit der EtherNet/IP-Fehlerhistorie für die Steuerung 1752-L24BBBE abgebildet ist.

Meldungen der Fehlerhistorie und erforderliche Maßnahmen

Mit den Meldungen der Fehlerhistorie können Sie Fehler erkennen und beheben.

Fehlermeldungen bei Steuerungssystemausfall

Meldung	Beschreibung	Erforderliche Maßnahmen
System Failure (Systemfehler)	Es ist ein Systemfehler aufgetreten.	Ersetzen Sie die Steuerung, wenn nach dem Aus- und Einschalten weiterhin ein Systemfehler gemeldet wird.
Invalid Configuration (Ungültige Konfiguration)	Die Konfiguration ist ungültig.	Die aktuelle Konfiguration weicht von der ursprünglichen Konfiguration ab. Prüfen Sie die Konfiguration, und ändern Sie sie entsprechend.

Programmierungsbezogene Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Function Block Status Error (Fehler des Funktionsblockstatus)	In den Einstellungsparameters des Funktionsblocks wurde ein inkompatibler Signaleingang als Eingangsbedingung gesetzt.	Überprüfen Sie die im Funktionsblock oder in der Programmierlogik eingegebenen Eingänge.

DeviceNet-Kommunikations-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Switch Setting Mismatch (Abweichung der Schaltereinstellungen)	Die Schaltereinstellungen stimmen nicht überein.	Vergewissern Sie sich, dass die Netzknotenadresse mit der Adresse in der letzten Konfiguration übereinstimmt. Ist dies nicht der Fall, ändern Sie sie auf die ursprüngliche Netzknotenadresse zurück, oder nehmen Sie die Konfiguration erneut vor. Wenn der Fehler erneut auftritt, ersetzen Sie die Steuerung.
Duplicate MAC ID (Doppelte MAC-ID)	Mindestens eine Netzknotenadresse wurde mehrfach verwendet.	Überprüfen Sie die Netzknotenadressen der anderen Netzknoten. Korrigieren Sie die Konfiguration so, dass jede Netzknotenadresse nur einmal verwendet wird, und schalten Sie die Stromversorgung aus und wieder ein.
Network PS Voltage Low (Versorgungsspannung des Netzwerks niedrig)	Die Versorgungsspannung des Netzwerks ist zu niedrig.	Stellen Sie sicher, dass die eingestellte Versorgungsspannung innerhalb des vorgeschriebenen Bereichs liegt. Vergewissern Sie sich, dass alle Kabel- und Leitungsverbindungen einwandfrei sind.

DeviceNet-Kommunikations-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Bus Off (Bus unterbrochen)	Die Kommunikation wurde aufgrund häufiger Datenfehler unterbrochen.	Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. Vergewissern Sie sich, dass sich an beiden Enden der Hauptleitung und nur dort ein Abschlusswiderstand befindet. Vergewissern Sie sich, dass im System keine starken Rauschstörungen vorliegen.
Transmission Timeout (Übertragungs-Timeout)	Bei der Übertragung ist ein Timeout aufgetreten.	
Standard I/O Connection Timeout (Timeout der Standard-E/A-Verbindung)	Bei der Standard-E/A-Verbindung ist ein Timeout aufgetreten.	
Relevant Safety I/O Communication Stopped Because of a Safety I/O Communication Error (Relevante Sicherheits-E/A-Kommunikation wurde aufgrund eines Fehlers bei der Sicherheits-E/A-Kommunikation unterbrochen)	Die entsprechende Sicherheits-E/A-Verbindung wurde aufgrund eines Timeouts der Sicherheits-E/A-Verbindung unterbrochen.	
All Safety I/O Communication Stopped Because of a Safety I/O Communication Error (Unterbrechung der gesamten Sicherheits-E/A-Kommunikation aufgrund eines Fehlers bei der Sicherheits-E/A-Kommunikation)	Sämtliche Sicherheits-E/A-Verbindungen wurden aufgrund eines Timeouts der Sicherheits-E/A-Verbindung unterbrochen.	
Timeout der Sicherheits-E/A-Verbindung	Bei der Sicherheits-E/A-Verbindung ist ein Timeout aufgetreten.	
Nonexistent Slave Device (Slave-Gerät nicht vorhanden)	Im System befindet sich kein Slave-Gerät.	
Safety I/O Connection Establishment Failure (Fehler beim Aufbau der Sicherheits-E/A-Verbindung)	Beim Herstellen einer Sicherheitsverbindung ist ein Fehler aufgetreten.	Stellen Sie sich, dass das Gerät ordnungsgemäß konfiguriert ist und betrieben wird.
Invalid Slave Device (Ungültiges Slave-Gerät)	Ein nicht autorisiertes Slave-Gerät befindet sich im Netzwerk (Überprüfungsfehler).	Überprüfen Sie das Slave-Gerät, und schließen Sie ein geeignetes Slave-Gerät an.
EM Transmission Error (Duplicate MAC ID) (EM-Übertragungsfehler (Doppelte MAC-ID))	Aufgrund einer doppelten Netzknotenadresse ist die Übertragung nicht möglich.	Überprüfen Sie die Netzknotenadressen der anderen Netzknoten. Korrigieren Sie die Konfiguration so, dass jede Netzknotenadresse nur einmal verwendet wird, und schalten Sie die Stromversorgung aus und wieder ein.
EM Transmission Error (Invalid Header) (EM-Übertragungsfehler (Ungültiger Header))	Aufgrund eines ungültigen Headers ist die Übertragung nicht möglich.	Überprüfen Sie die Netzknotenadresse, die Klassen-ID und die Instanz-ID der zu übertragenden Nachricht.
EM Transmission Error (Device Offline) (EM-Übertragungsfehler (Gerät offline))	Da sich das zentrale Gerät nicht im Netzwerk befindet, ist die Übertragung nicht möglich.	Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. Vergewissern Sie sich, dass sich an beiden Enden der Hauptleitung und nur dort ein Abschlusswiderstand befindet. Ergreifen Sie Maßnahmen gegen starke Störungen. Stellen Sie sicher, dass die eingestellte Versorgungsspannung für die Stromversorgung des Netzwerks innerhalb des vorgeschriebenen Bereichs liegt.
EM Transmission Error (Message ID Error (EM-Übertragungsfehler (Fehler der Nachrichten-ID))	Aufgrund eines Nachrichten-ID-Fehlers ist die Übertragung nicht möglich.	
EM Transmission Error (Response Timeout) (EM-Übertragungsfehler (Antwort-Timeout))	Aufgrund eines Antwort-Timeouts ist die Übertragung nicht möglich.	

DeviceNet-Kommunikations-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
EM Transmission Error (Destination Device Absence) (EM-Übertragungsfehler (Zielgerät nicht vorhanden))	Da sich das Zielgerät nicht im Netzwerk befindet, ist die Übertragung nicht möglich.	Überprüfen Sie die Netzknotenadresse der Zielknotens und die Netzknotenadresse der zu übertragenden Nachricht. Stellen Sie sicher, dass die eingestellte Versorgungsspannung für den Zielnetzknoten innerhalb des vorgeschriebenen Bereichs liegt. Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. Vergewissern Sie sich, dass sich an beiden Enden der Hauptleitung und nur dort ein Abschlusswiderstand befindet. Ergreifen Sie Maßnahmen gegen starke Störungen.
EM Transmission Error (Destination Buffer Full) (EM-Übertragungsfehler (Zielpuffer belegt))	Da der Zielpuffer belegt war, konnte die Übertragung nicht durchgeführt werden.	Überprüfen Sie die Nachrichtenempfangsgröße des Zielnetzknotens.
EM Transmission Error (Command Length Error) (EM-Übertragungsfehler (Fehler der Befehlslänge))	Da der Befehl länger als die maximal zulässige Länge war, konnte die Übertragung nicht durchgeführt werden.	Überprüfen Sie die Größe der Antwortnachricht des Ziels. Überprüfen Sie außerdem, ob die in der Anfragenachricht erwartete Antwortgröße korrekt ist.
EM Transmission Error (New Request Received) (EM-Übertragungsfehler (Neue Anfrage empfangen))	Die Nachricht wurde gelöscht, da eine neue Anfrage empfangen wurde.	Keine.
Received Error Response (Empfangene Fehlerantwort) (UEM)	Es wurde eine Fehlerantwort empfangen, während die Anwenderfunktion für explizite Nachrichten verwendet wurde.	Vergewissern Sie sich, dass die angegebene Dienst- oder Datengröße in der expliziten Nachricht mit den Spezifikationen des Zielobjekts übereinstimmt.

Fehlermeldungen beim Ausfall des EtherNet/IP-Steuerungssystems

Meldung	Beschreibung	Erforderliche Maßnahmen
System Failure (Systemfehler)	Es ist ein Systemfehler aufgetreten.	Schalten Sie die Stromversorgung aus und wieder ein. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
	Es ist ein EtherNet/IP-Speicherfehler aufgetreten.	
	Es ist ein Fehler der EtherNet/IP-Kommunikationssteuerung aufgetreten.	
	Dieselbe IP-Adresse ist bereits für ein anderes Gerät im Netzwerk festgelegt.	Überprüfen Sie die IP-Adressen der anderen Geräte und legen Sie eine Adresse fest, die noch nicht verwendet wird.
	Es ist ein Logikfehler in der Einstellungstabelle aufgetreten.	Überprüfen Sie die Konfiguration. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
	Es ist ein Verbindungsfehler mit dem BOOTP-Server aufgetreten.	Stellen Sie sicher, dass das Kabel richtig angeschlossen ist. Stellen Sie sicher, dass der BOOTP-Server normal arbeitet.
	Es ist ein Logikfehler der EtherNet/IP-Basiseinstellung aufgetreten.	Überprüfen Sie die Konfiguration. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
	Es ist ein Kommunikationsfehler des EtherNet/IP-Standardziels aufgetreten.	Stellen Sie sicher, dass dieselben Kommunikationseinstellungen für jeden Netzknoten verwendet werden. Vergewissern Sie sich, dass die Kabel nicht abgezogen oder verbogen sind. Stellen Sie sicher, dass der Master mit Strom versorgt wird.
	Es ist ein Fehler aufgrund einer unterbrochenen Verbindung aufgetreten.	Stellen Sie sicher, dass dieselben Kommunikationseinstellungen für jeden Netzknoten verwendet werden. Vergewissern Sie sich, dass die Kabel nicht abgezogen oder verbogen sind. Stellen Sie sicher, dass der Hub mit Strom versorgt wird.

Auf die E/A-Stromversorgung bezogene Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Input PS Voltage Low (Eingangsspannungsversorgung niedrig)	Die E/A-Stromversorgung (V1, G1) ist nicht angeschlossen.	Stellen Sie sicher, dass die eingestellte Versorgungsspannung innerhalb des vorgeschriebenen Bereichs liegt. Vergewissern Sie sich, dass alle Kabel- und Leitungsverbindungen einwandfrei sind.
Output PS Voltage Low (Ausgangsspannungsversorgung niedrig)	Die E/A-Stromversorgung (V2, G2) ist nicht angeschlossen.	

Sicherheitseingangs-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
External Test Signal Failure at Safety Input (Fehler des externen Testsignals am Sicherheitseingang)	In der externen Verdrahtung des Sicherheitseingangs ist ein Fehler aufgetreten.	Vergewissern Sie sich, dass das Eingangssignalkabel keinen Kontakt zur Stromquelle (positive Seite) hat. Vergewissern Sie sich, dass am Eingangsignalkabel kein Erdschluss vorliegt. Vergewissern Sie sich, dass die Verbindung des Eingangssignalkabels einwandfrei ist. Vergewissern Sie sich, dass kein Kurzschluss zwischen den Eingangssignalleitungen vorliegt. Vergewissern Sie sich, dass kein Fehler im angeschlossenen Gerät vorliegt. Stellen Sie sicher, dass der konfigurierte Wert der Diskrepanzzeit gültig ist. Dieser Fehlerstatus wird gelöscht, wenn die Fehlerzeit für die Eingangsverriegelung abgelaufen und die Fehlerursache bis dahin behoben ist. Die Zielsicherheitseingänge müssen ausgeschaltet sein. Zum Ändern der Diskrepanzzeit müssen Sie den Sicherheitseingang neu konfigurieren.
Discrepancy Error at Safety Input (Diskrepanzfehler am Sicherheitseingang)	Zwischen zwei für den Zweikanalmodus konfigurierten Eingängen liegt eine Diskrepanz vor.	
Internal Input Failure at Safety Input (Interner Eingangsfehler am Sicherheitseingang)	Am Sicherheitseingang wurde ein interner Schaltkreisfehler registriert.	Ersetzen Sie das Gerät, wenn nach dem Aus- und Einschalten der Stromversorgung weiterhin ein Systemfehler gemeldet wird.

Testausgangs-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Overload Detected at Test Output (Überlast am Testausgang festgestellt)	Am Testausgang fließt ein zu hoher Strom.	Überprüfen Sie, ob das Ausgangsignal einen Erdschluss aufweist oder überlastet ist.
Stuck-at-high Detected at Test Output (Blockierung im Ein-Zustand am Testausgang festgestellt)	Ein Testausgang ist im eingeschalteten Zustand blockiert.	Überprüfen Sie, ob die Stromquelle eine Verbindung zum Ausgangssignalkabel hat. Schalten Sie den Eingang aus, sobald die Fehlerzeit für die Eingangsverriegelung abgelaufen ist und die Fehlerursache behoben wurde. Der Fehler wird dann zurückgesetzt. Wenn kein Fehler bei der Verdrahtung vorliegt, tauschen Sie das Gerät aus.
Under-current Detected Using Muting Lamp (Unterstrombedingung mittels Muting-Lampe festgestellt)	Am Testausgang T3 ist ein Fehler durch Unterschreitung der unteren Stromgrenze aufgetreten.	Überprüfen Sie, ob das Ausgangssignalkabel sich gelöst hat oder ob die Muting-Lampe ausgebrannt ist. Wenn kein Fehler bei der Verdrahtung vorliegt, überprüfen Sie die Statusanzeigen.

Sicherheitsausgangs-Fehlermeldungen

Meldung	Beschreibung	Erforderliche Maßnahmen
Over Current Detected at Safety Output (Überstrom am Sicherheitsausgang festgestellt)	Am Sicherheitsausgang wurde ein Überstrom festgestellt.	Stellen Sie sicher, dass am Ausgang kein Überstrom vorliegt. Vergewissern Sie sich, dass am Ausgangsignalkabel kein Erdschluss vorliegt. Vergewissern Sie sich, dass das Ausgangssignalkabel keinen Kontakt zur Stromquelle (positive Seite) hat. Vergewissern Sie sich, dass kein Kurzschluss zwischen den Ausgangssignalleitungen vorliegt.
Short Circuit Detected at Safety Output (Kurzschluss am Sicherheitsausgang festgestellt)	Am Sicherheitsausgang wurde ein Kurzschluss festgestellt.	
Stuck-at-high Detected at Safety Output (Blockierung im Ein-Zustand am Sicherheitsausgang festgestellt)	Ein Sicherheitsausgang ist im eingeschalteten Zustand blockiert.	
Cross Connection Detected at Safety Output (Querverbindung am Sicherheitsausgang festgestellt)	Zwischen den Ausgangssignalkabeln an einem Sicherheitsausgang wurde ein Kurzschluss festgestellt.	
Dual Channel Violation at Safety Output (Zweikanalfehler am Sicherheitsausgang)	An einem Sicherheitsausgang wurde ein Ausgangsdatenfehler registriert.	Überprüfen Sie, ob die Daten der beiden Ausgänge im Zweikanalmodus als äquivalente Kanäle konfiguriert sind.

Download-Fehler und Abhilfemaßnahmen

Die Steuerung gibt beim Herunterladen von Konfigurationsdaten in die Steuerung eventuell eine Fehlerantwort zurück. Zum Identifizieren des Fehlers können Sie die in der Software RSNetWorx for DeviceNet angezeigten Meldungen verwenden.

Download-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
Cannot be executed in the current mode. (Keine Ausführung im aktuellen Modus möglich.)	Ein kritischer Fehler (Abbruch) ist aufgetreten, und die MS-Anzeige blinkt rot.	Überprüfen Sie, ob die Schalter richtig eingestellt sind. Setzen Sie das System andernfalls zurück, um die Konfigurationsdaten zu löschen.
The device is locked. (Das Gerät ist blockiert.)	Die Konfiguration ist gesperrt und die LOCK-Statusanzeige leuchtet.	Heben Sie die Verriegelung des Geräts auf.
The TUNID is different. (Die TUNID stimmt nicht überein.)	Die Sicherheitsnetzwerknummer (SNN) wurde seit dem Zurücksetzen des Geräts (die NS-Statusanzeige blinkt grün und rot) nicht festgelegt oder die SNN im Gerät stimmt nicht mit der von RSNetWorx for DeviceNet heruntergeladenen SNN überein.	1. Setzen Sie das Gerät auf die Standardeinstellungen zurück, und laden Sie die Parameter erneut herunter. Die SNN unterschiedet sich möglicherweise von anderen Geräten. Wenn auf der alphanumerischen Anzeige der Steuerung „d6“ angezeigt wird und in der Tabelle mit der Fehlerhistorie die Meldung „Safety I/O Connection Establishment Failure“ (Fehler beim Herstellen der Sicherheits-E/A-Verbindung) erscheint, nachdem der Betriebsmodus geändert wurde, fahren Sie mit dem nächsten Schritt fort. 2. Wählen Sie in RSNetWorx for DeviceNet die Option „Network > Upload“ (Netzwerk > Hochladen). Vereinheitlichen Sie die SNN im ganzen Netzwerk, und setzen Sie alle Geräte auf die Standardeinstellungen zurück. Laden Sie nach dem Zurücksetzen die Parameter wieder in die Geräte herunter.
Privilege violation. (Berechtigungsfehler.)	1. Das verwendete Kennwort ist nicht mit der Berechtigung zum Ändern der Konfiguration ausgestattet. 2. Es wurde versucht, über eine DeviceNet-Verbindung in den eigenständigen Modus zu wechseln.	1. Vergewissern Sie sich, dass Sie das richtige Kennwort verwenden. 2. Stellen Sie über den USB-Anschluss eine Verbindung zur SmartGuard-Steuerung her, und laden Sie die Konfiguration erneut herunter. Bei der Steuerung 1752-L24BBBE können Sie die Konfiguration auch über das EtherNet/IP-Netzwerk herunterladen.
Cannot be executed in the current device mode. (Ausführung im aktuellen Gerätemodus nicht möglich.)	Daten werden von mehr als einer Instanz der Software RSNetWorx for DeviceNet heruntergeladen.	Warten Sie, bis der Download-Vorgang von der anderen Instanz abgeschlossen ist.

Download-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
An error was found during parameter check. (Während der Parameterprüfung wurde ein Fehler festgestellt.)	Zwischen den Konfigurationsparametern liegt eine Inkonsistenz vor.	Stellen Sie die Parametereinstellungen richtig. Suchen Sie nach folgenden Problemen: • Ein konfigurierter Zeitparameter für einen Funktionsblock ist kürzer als die Zykluszeit der Steuerung. • Das angeforderte Paketintervall (RPI) für eine Sicherheitsverbindung ist kürzer als die Zykluszeit. • Ein Sicherheitseingang ist als „Used with test pulse“ (Mit Testimpuls verwendet) konfiguriert, jedoch ist keine Testquelle festgelegt. • Beim Konfigurieren der Sicherheitseingänge für den Zweikanalmodus wurde ein Eingang als Standardeingang konfiguriert, der andere weist jedoch eine andere Einstellung auf. • Beim Konfigurieren der Sicherheitseingänge für den Zweikanalmodus wurde ein Eingang als nicht verwendet eingestellt, der andere weist jedoch eine andere Einstellung auf. • Beim Konfigurieren der Sicherheitsausgänge für den Zweikanalmodus wurde ein Ausgang als nicht verwendet eingestellt, der andere weist jedoch eine andere Einstellung auf. • Bei der Sicherheits-E/A-Konfiguration wurde eine Einstellung vorgenommen, durch die die maximale Anzahl der vom Master verwalteten Verbindungs-IDs (12) überschritten wurde. Klicken Sie im Dialogfeld „Safety Connection Properties“ (Eigenschaften der Sicherheitsverbindung) auf „Advanced“ (Erweitert). Aktivieren Sie das Kontrollkästchen „Request target device to allocate message IDs“ (Zielgerät zur Zuweisung der Meldungs-IDs anfordern).
The data used by the logic program is not aligned with other data. (Die vom Logikprogramm verwendeten Daten stimmen nicht mit den anderen Daten überein.)	Durch eine Änderung der Netzwerkkonfiguration weichen die Daten der Programmierlogik von den anderen Daten ab.	Überprüfen Sie mit dem Logik-Editor die geänderten E/A-Speicherorte, und setzen Sie die Daten zurück.
Could not access the device. (Auf das Gerät konnte nicht zugegriffen werden.)	Die Steuerung wurde während eines Downloads von einem anderen Netzknoten zurückgesetzt, und die Sicherheitsnetzwerknummer (SNN) wurde noch nicht eingestellt. Die NS-Statusanzeige blinkt rot/grün.	Stellen Sie die SNN ein, und laden Sie die Daten erneut herunter.
Could not open connection. (Verbindung konnte nicht geöffnet werden.)	Beim Herunterladen auf die Steuerung über das DeviceNet- oder EtherNet/IP-Netzwerk konnte keine Verbindung zur Steuerung hergestellt werden.	1. Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit Strom versorgt wird, und versuchen Sie erneut, die Daten herunterzuladen. 2. Ändern Sie den Betriebsmodus der Sicherheits-Masters auf Leerlauf. 3. Es ist ebenfalls möglich, dass durch Störungen oder andere Faktoren die Kommunikation instabil geworden ist. • Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. • Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. • Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. • Vergewissern Sie sich, dass beide Enden der Hauptleitung Abschlusswiderstände aufweisen. • Ergreifen Sie Maßnahmen gegen starke Störungen.

Download-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
Message could not be sent. (Nachricht konnte nicht gesendet werden.)	Beim Herunterladen auf die Steuerung über den USB-Anschluss oder das EtherNet/IP-Netzwerk konnte keine Verbindung zur Steuerung hergestellt werden.	Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit Strom versorgt wird, und versuchen Sie erneut, die Daten herunterzuladen.
Connection failed. (Verbindung abgebrochen.)	Es wurde versucht, ein Gerät im DeviceNet- oder EtherNet/IP-Netzwerk über den USB-Anschluss zu konfigurieren, dies war jedoch nicht möglich.	Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit Strom versorgt wird, und versuchen Sie erneut, die Daten herunterzuladen. Es ist ebenfalls möglich, dass durch Störungen oder andere Faktoren die Kommunikation instabil geworden ist. • Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. • Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. • Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. • Vergewissern Sie sich, dass beide Enden der Hauptleitung Abschlusswiderstände aufweisen. • Ergreifen Sie Maßnahmen gegen starke Störungen.
Program incomplete. (Programm unvollständig.) Start Logic Editor and check program. (Logik-Editor starten und Programm überprüfen.)	In einem im Logikprogramm verwendeten Funktionsblock sind offene Ein- oder Ausgänge vorhanden.	Verbinden Sie im Logik-Editor der Software RSNetWorx for DeviceNet die offenen Eingänge bzw. Ausgänge, oder ändern Sie die Anzahl der E/A für den Funktionsblock, um die nicht verbundenen Ein- oder Ausgänge zu löschen.

Rücksetzfehler und Abhilfemaßnahmen

Die Steuerung gibt beim Zurücksetzen möglicherweise eine Fehlerantwort zurück. Zum Identifizieren des Fehlers können Sie die in der Software RSNetWorx for DeviceNet angezeigten Meldungen verwenden.

Rücksetz-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
Cannot execute in current mode. (Ausführung im aktuellen Modus nicht möglich.)	Der angegebene Rücksetzvorgang kann im derzeitigen Zustand der Steuerung nicht durchgeführt werden.	Wechseln Sie die Betriebsart oder den Konfigurationsverriegelungsstatus, und führen Sie den Rücksetzvorgang dann durch.
The device has a different TUNID. the device TUNID will be used to reset. (Die TUNID des Geräts stimmt nicht überein. Die Geräte-TUNID wird für den Rücksetzvorgang verwendet.) Is that OK? (Ist das OK?)	Die im Gerät gespeicherte Sicherheitsnetzwerknummer (SNN) stimmt nicht mit der SNN überein, die von RSNetWorx for DeviceNet angegeben wurde.	Überprüfen Sie, ob die MAC-ID des Geräts übereinstimmt. Wenn die MAC-ID übereinstimmt und Sie den Rücksetzvorgang mit der im Gerät gespeicherten SNN durchführen möchten, fahren Sie mit dem Rücksetzen fort.

Rücksetz-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
Access error. (Zugriffsfehler.)	Das verwendete Kennwort weist nicht die Berechtigung zum Ändern von Konfigurationen auf.	Stellen Sie sicher, dass Sie das richtige Kennwort verwenden.
The device cannot be accessed or the device type or password is different. (Auf das Gerät kann nicht zugegriffen werden, oder der Gerätetyp oder das Kennwort stimmen nicht überein.)	1. Das Gerät wurde soeben zurückgesetzt oder die Stromversorgung wurde aus- und eingeschaltet und das Gerät ist noch nicht für die Kommunikation bereit.	1. Vergewissern Sie sich, dass das Gerät zur Kommunikation bereit ist, und versuchen Sie erneut, den Rücksetzvorgang durchzuführen.
	2. Möglicherweise unterstützt das angegebene Gerät den Rücksetzvorgang nicht.	2. Vergewissern Sie sich, dass die MAC-ID des Geräts richtig ist.
	3. Die Konfigurationsdaten sind verriegelt. Die LOCK-Statusanzeige leuchtet.	3. Entfernen Sie die Verriegelung, und führen Sie den angegebenen Rücksetzvorgang durch.
	4. Das Gerät führt Sicherheits-E/A-Kommunikation durch und kann die angegebene Anforderung nicht durchführen.	4. Ändern Sie den Betriebsmodus des entsprechenden Sicherheits-Masters auf Leerlauf, und führen Sie den angegebenen Rücksetzvorgang durch.
Connection failed. (Verbindung abgebrochen.)	Es wurde versucht, ein Gerät im DeviceNet- oder EtherNet/IP-Netzwerk über den USB-Anschluss zurückzusetzen, dies war jedoch nicht möglich.	Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit Strom versorgt wird, und versuchen Sie erneut, den Rücksetzvorgang durchzuführen. Es ist ebenfalls möglich, dass durch Störungen oder andere Faktoren die Kommunikation instabil geworden ist. • Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. • Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. • Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. • Vergewissern Sie sich, dass beide Enden der Hauptleitung Abschlusswiderstände aufweisen. • Ergreifen Sie Maßnahmen gegen starke Störungen.

Modusänderungsfehler und Abhilfemaßnahmen

Die Steuerung gibt beim Ändern des Modus möglicherweise eine Fehlerantwort zurück. Zum Identifizieren des Fehlers können Sie die in der Software RSNetWorx for DeviceNet angezeigten Meldungen verwenden.

Modusänderungs-Fehlermeldungen von RSNetWorx for DeviceNet und Abhilfemaßnahmen

Meldung	Beschreibung	Erforderliche Maßnahmen
Cannot be executed in the current mode. (Keine Ausführung im aktuellen Modus möglich.)	1. Das Gerät wurde nicht konfiguriert. 2. Ein kritischer Fehler (Abbruch) ist aufgetreten.	1. Laden Sie die Geräteparameter herunter. 2. Stellen Sie die Schalter des Geräts richtig ein, oder führen Sie einen Rücksetzvorgang durch, um die Konfigurationsdaten zu löschen, und laden Sie die Geräteparameter erneut herunter.
Already set to the specified mode. (Bereits im angegebenen Modus eingestellt.)	Das Gerät befindet sich bereits im angegebenen Modus.	
The device has a different TUNID. (Die TUNID des Geräts stimmt nicht überein.)	Die im Gerät gespeicherte Sicherheitsnetzwerknummer (SNN) stimmt nicht mit der SNN überein, die von RSNetWorx for DeviceNet angegeben wurde.	Vergewissern Sie sich, dass die MAC-ID des Geräts übereinstimmt. Wenn sie übereinstimmt, entspricht die Netzwerkadresse des Geräts nicht der Netzwerkadresse in der Konfigurationsdatei von RSNetWorx for DeviceNet. Laden Sie das Netzwerk in die Software RSNetWorx for DeviceNet hoch, sodass die Netzwerkadressen übereinstimmen.
Access error. (Zugriffsfehler.)	Das verwendete Kennwort weist nicht die Berechtigung zum Ändern des Betriebsmodus auf.	Stellen Sie sicher, dass Sie das richtige Kennwort verwenden.
The device cannot be accessed, or the device type or password is different. (Auf das Gerät kann nicht zugegriffen werden, oder der Gerätetyp oder das Kennwort stimmen nicht überein.)	1. Das Gerät wurde soeben zurückgesetzt oder die Stromversorgung wurde aus- und eingeschaltet und das Gerät ist noch nicht für die Kommunikation bereit. 2. Das Gerät, für das die Modusänderung angefordert wurde, unterstützt diese möglicherweise nicht.	1. Vergewissern Sie sich, dass das Gerät zur Kommunikation bereit ist, und versuchen Sie erneut, den Modus zu ändern. 2. Vergewissern Sie sich, dass die MAC-ID des Geräts richtig ist.
Connection failed. (Verbindung abgebrochen.)	Es wurde versucht, die Betriebsart eines Geräts im DeviceNet- oder EtherNet/IP-Netzwerk über den USB-Anschluss zu ändern, dies war jedoch nicht möglich.	Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit Strom versorgt wird, und versuchen Sie erneut, den Modus zu ändern. Es ist ebenfalls möglich, dass durch Störungen oder andere Faktoren die Kommunikation instabil geworden ist. • Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. • Stellen Sie sicher, dass die Kabel der Haupt- und Zweigleitungen nicht zu lang sind. • Vergewissern Sie sich, dass alle Kabel und Leitungen fest verbunden sind. • Vergewissern Sie sich, dass beide Enden der Hauptleitung Abschlusswiderstände aufweisen. • Ergreifen Sie Maßnahmen gegen starke Störungen.

Steuerungsspezifikationen

Einleitung

Dieser Anhang enthält Spezifikationsdaten für die Steuerung SmartGuard 600.

Thema	Seite
Allgemeine Spezifikationen	201
Umgebungsspezifikationen	203
Zertifizierungen	205

Allgemeine Spezifikationen

Attribute	1752-L24BBB	1752-L24BBBE
Abmessungen (HxBxT), ca.	99,0[4] x 99,4 x 131,4 mm[5]	99,0[4] x 113,0 x 131,4 mm[5]
Gewicht, ca.	460 g	575 g
DeviceNet-Stromlast, max.	15 mA bei 24 V DC	
Netzspannung[1]	20,4 bis 26,4 V DC (24 V DC, –15 bis 10 %)	
Einschaltstrom – Gerätenetzteil	4,8 A Spitze für 600 µs bei V0/G0	
Einschaltstrom – Sicherheitseingangs-Netzteil	2,6 A Spitze für 3 ms bei V1/G1	
DeviceNet-Spannungsbereich	11 bis 25 V DC	
Stromverbrauch (V0 – interner Logikschaltkreis)	230 mA bei 24 V DC	280 mA bei 24 V DC
Überlastschutz	Abschalten des betroffenen Ausgangs mit zyklischer Neuverbindung	
Isolationsspannung	50 V, funktionaler Isolationstyp Getestet bei 600 V AC für 60 s, zwischen allen Gruppen	
Drahttyp	Kupfer	
Verdrahtungskategorie[2]	2 – an Strom-, Signal- und Kommunikationsanschlüssen	2 – an Leistungs-, 1 – an Signal-, 1 – an Kommunikationsanschlüssen
Leiterquerschnitt	Verwenden Sie für das Netzteil und die Ein-/Ausgänge massive Drähte mit 0,2 bis 2,5 mm^2 (AWG 12 bis 24) oder flexible Standarddrähte mit 0,34 bis 1,5 mm^2 (AWG 16 bis 22). Bereiten Sie Standarddrähte vor dem Verdrahten vor, indem Sie diese mit Terminierungshülsen mit Kunststoffisolierung (kompatibel mit der Norm DIN 46228-4) versehen. Für Ethernet-Verbindungen: RJ45-Anschluss gemäß IEC 60603-7, 2 oder 4 Paare, Kategorie 5e Minimale Kabelanforderung gemäß TIA 569-B.1 oder Kabel der Kategorie 5 gemäß ISO/IEC 24701	
Anzugsmoment der E/A-Klemmenschrauben	0,56 bis 0,79 Nm	

Attribute	**1752-L24BBB**	**1752-L24BBBE**
Nordamerikanischer Temperaturcode	T4A	
Eingangstyp	Stromsenke	
Eingangsspannung im EIN-Zustand, min.	11 V DC	
Eingangsspannung im AUS-Zustand, max.	5 V DC	
Eingangsstrom im AUS-Zustand, max.	1 mA	
Eingangsstrom	4,5 mA	
Eingangsimpedanz	2,6 kΩ	
Testausgangstyp	Stromquelle	
Ausgangsstrom, Impulstest(3)	0,7 A	
Stoßstrom, Testausgang	0,7 A	
Spannung im AUS-Zustand, Impulstest max.	1,2 V	
Ausgangsleckstrom, Impulstest, max.	0,1 mA	
Ausgangsstrom für Muting-Lampe (T3) • Mehr als 25 mA • Weniger als 5 mA	• Normaler Betrieb (zur Vermeidung von Fehlern bei Verwendung als Muting-Lampenausgang) • Fehler (bei Verwendung als Muting-Lampenausgang wird eine Fehleranzeige generiert)	
Ausgangstyp	Stromquelle	
Ausgangsstrom	0,5 A	
Ausgangsstoßstrom	0,5 A	
Ausgangsspannung im AUS-Zustand, max.	1,2 V	
Eingangsleckstrom im AUS-Zustand, max.	0,1 mA	
Wärmeabstrahlung	9,3 W unter max. Last	

Attribute	1752-L24BBB	1752-L24BBBE
Ethernet-Kommunikation		
CIP-Verbindungen	Nicht anwendbar	2
Automatische Verhandlung	Nicht anwendbar	Unterstützt
Datenrate	Nicht anwendbar	10/100 Mbit/s
Duplex	Nicht anwendbar	Voll/Halb
Übertragungsleistung der Einheit	Nicht anwendbar	3000 pps(6)
Kommunikation expliziter Nachrichten	Nicht anwendbar	502 Byte(7)

(1) V0/G0 für internen Logikschaltkreis; V1/G1 für externe Eingangsgeräte und Testausgänge; V2/G2 für externe Ausgangsgeräte.

(2) Planen Sie mithilfe dieser Informationen zur Leitungskategorie die Verlegung der Leiter. Siehe die Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1.

(3) T0 bis T3 Gesamtstrom zur selben Zeit: 1,4 A.

(4) Bei der Höhenangabe wurden die Klemmenanschlüsse berücksichtigt.

(5) Bei der Tiefenangabe wurde der DeviceNet-Anschluss berücksichtigt.

(6) PPS = Pakete pro Sekunde. Gibt die Anzahl der Sende- oder Empfangspakete an, die pro Sekunde verarbeitet werden können.

(7) Die maximale Nachrichtenlänge für eine Verbindung der Klasse 3 und eine UCMM-Verbindung.

Umgebungsspezifikationen

Attribute	1752-L24BBB	1752-L24BBBE
Temperatur, Lagerung	IEC 60068-2-1 (Test Ab, ohne Verpackung, außer Betrieb, kalt), IEC 60068-2-2 (Test Bb, ohne Verpackung, außer Betrieb, trockene Hitze), IEC 60068-2-14 (Test Na, ohne Verpackung, außer Betrieb, Temperaturschock): –40 bis 70 °C	
Temperatur, Betrieb	IEC 60068-2-1 (Test Ad, in Betrieb, kalt), IEC 60068-2-2 (Test Bd, in Betrieb, trockene Hitze), IEC 60068-2-14 (Test Nb, in Betrieb, Temperaturschock): –10 bis 55 °C	
Relative Luftfeuchtigkeit	IEC 60068-2-30 (Test Db, ohne Verpackung, außer Betrieb, feuchte Hitze): 10 bis 95 %, nicht kondensierend	
Vibration	IEC 60068-2-6 (Test Fc, in Betrieb): 0,35 mm bei 10 bis 57 Hz 5 g bis 57 bis 150 Hz	IEC 60068-2-6 (Test Fc, in Betrieb): 5 g bis 10 bis 500 Hz
Stoßeinwirkung, in Betrieb	IEC 60068-2-27 (Test Ea, ohne Verpackung, Stoßeinwirkung): 15 g	
Stoßeinwirkung, außer Betrieb	IEC 60068-2-27 (Test Ea, ohne Verpackung, Stoßeinwirkung): 30 g	
Gehäuse-Schutzart	Erfüllt IP20	
Emissionen	CISPR 11: Gruppe 1, Klasse A	
Störfestigkeit	IEC 61000-4-2: • 4 kV Kontaktentladungen • 8 kV Luftentladungen	IEC 61000-4-2: • 6 kV Kontaktentladungen • 8 kV Luftentladungen

Attribute	1752-L24BBB	1752-L24BBBE
Störfestigkeit gegenüber HF-Strahlung	IEC 61000-4-3: • 10 V/m mit 1 kHz Sinuskurve 80 % AM von 80 bis 1000 MHz • 10 V/m mit 1 kHz Sinuskurve 80 % AM von 1,4 bis 2,0 GHz • 10 V/m mit 200 Hz 50 % Impuls 100 % AM bei 900 MHz • 10 V/m mit 200 Hz 50 % Impuls 100 % AM bei 1200 MHz • 3 V/m mit 1 kHz Sinuskurve 80 % AM von 2000 bis 2700 MHz	IEC 61000-4-3: • 10 V/m mit 1 kHz Sinuskurve 80 % AM von 80 bis 1000 MHz • 10 V/m mit 1 kHz Sinuskurve 80 % AM von 1,4 bis 2,0 GHz • 20 V/m mit 200 Hz 50 % Impuls 100 % AM bei 800, 900, 1200 MHz • 3 V/m mit 1 kHz Sinuskurve 80 % AM von 2000 bis 2700 MHz
EFT/B-Störfestigkeit	IEC 61000-4-4: • ±2 kV bei 5 kHz an Leistungsanschlüssen • ±2 kV bei 5 kHz an Signalanschlüssen • ±2 kV bei 5 kHz an Kommunikationsanschlüssen	IEC 61000-4-4: • ±2 kV bei 5 kHz an Leistungsanschlüssen • ±1 kV bei 5 kHz an Signalanschlüssen • ±1 kV bei 5 kHz an Kommunikationsanschlüssen
Überspannungsstörfestigkeit	IEC 61000-4-5: • ±1 kV Netz-Netz (DM) und ±2 kV Netz-Erdung (CM) an Leistungsanschlüssen • ±1 kV Netz-Netz (DM) und ±2 kV Netz-Erdung (CM) an Signalanschlüssen • ±1 kV Netz-Erdung (CM) an Kommunikationsanschlüssen	IEC 61000-4-5: • ±500 V Netz-Netz (DM) und ±1 kV Netz-Erdung (CM) an Leistungsanschlüssen • ±1 kV Netz-Erdung (CM) an Signalanschlüssen • ±1 kV Netz-Erdung (CM) an Kommunikationsanschlüssen
Störfestigkeit gegenüber leitungsgeführten HF-Störgrößen	IEC 61000-4-6: • 10 V eff. mit 1 kHz Sinuskurve 80 % AM von 150 kHz bis 80 MHz	

Zertifizierungen

Zertifizierung[1] (wenn Produkt entsprechend gekennzeichnet ist)	**Wert**
c-UL-us	UL-Auflistung für explosionsgefährdete Bereiche der Klasse I, Division 2, Gruppe A, B, C, D, zertifiziert für die USA und Kanada. Siehe UL-Datei E194810
CE	EMV-Richtlinie der Europäischen Union 2004/108/EEC, konform mit: • EN 61000-6-4; Störaussendung für Industriebereiche • EN 61131-2; Speicherprogrammierbare Steuerungen (Absatz 8, Zone A und B) • EN 61326-1; Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen • EN 61000-6-2; Störfestigkeit für Industriebereiche
C-Tick	Australian Radiocommunications Act, konform mit: AS/NZS CISPR 11; Industrielle Emissionen
TÜV	TÜV-Zertifizierung für funktionale Sicherheit Funktionale Sicherheit: SIL 1 bis 3, gemäß IEC 61508; Performance Level PL(e) gemäß ISO 13849-1, Kategorie 1 bis 4, gemäß EN954-1; NFPA79
UL	UL-Zertifizierung für funktionale Sicherheit. Siehe UL-Datei E256621
ODVA	ODVA-Konformität getestet gemäß den DeviceNet- und Ethernet/IP-Spezifikationen

(1) Konformitätserklärungen, Zertifikate und weitere Zertifizierungsdetails erhalten Sie über den Link zur Produktzertifizierung (Product Certification) unter http://ab.com.

Notizen:

Statusanzeigen

Einleitung

Thema	Seite
Modulstatusanzeigen	207
Fehleridentifikation mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige	213
Identifikation von EtherNet/IP-Fehlern mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige	218

Modulstatusanzeigen

In der folgenden Tabelle werden die verschiedenen Farb- und Zustandskombinationen der Statusanzeigen erläutert. Überprüfen Sie anhand dieser Tabelle, ob ggf. Korrekturmaßnahmen erforderlich sind.

ACHTUNG

Statusanzeigen sind keine zuverlässigen Anzeigen für Sicherheitsfunktionen. Sie sollten ausschließlich für allgemeine Diagnosen während der Inbetriebnahme und Fehlerbeseitigung verwendet werden. Verwenden Sie Statusanzeigen nicht als Indikatoren für den Betriebszustand.

Beschreibung der Modulstatusanzeige (MS)

Zustand der Modulstatusanzeige	Bedeutung	Maßnahme
Aus	Keine Stromversorgung.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Grün, ein	Die Steuerung befindet sich im Betriebsmodus „Run“ (Betrieb) und arbeitet normal.	Keine Maßnahme erforderlich.
Grün, blinkend	Die Steuerung befindet sich im Modus „Idle“ (Leerlauf).	
Rot, blinkend	Ein behebbarer Fehler liegt vor.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Rot, ein	Ein nicht behebbarer Fehler liegt vor.	
Rot/Grün, blinkend	Selbsttest wird durchgeführt. Oder, die Steuerungskonfiguration wird derzeit heruntergeladen oder ist unvollständig oder fehlerhaft. Beispiel: Die Netzwerk-ID (UNID) wurde nicht angegeben.	

Wenn die Modulstatusanzeige aus ist, gehen Sie wie folgt vor.

1. Schalten Sie die Stromversorgung aus und wieder ein.
2. Überprüfen Sie, ob Störungen die Stromversorgung beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen.
3. Wenden Sie sich an Rockwell Automation.

Wenn die Modulstatusanzeige rot blinkt, gehen Sie wie folgt vor.

1. Überprüfen Sie die korrekte Konfiguration der Schalter.
2. Setzen Sie die Konfigurationsdaten zurück.

Wenn die Modulstatusanzeige konstant rot leuchtet (EIN), gehen Sie wie folgt vor.

1. Schalten Sie die Stromversorgung aus und wieder ein.
2. Überprüfen Sie die externe Verdrahtung.
3. Überprüfen Sie, ob Störungen die Stromversorgung beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen.
4. Wenden Sie sich an Rockwell Automation.

Wenn die Modulstatusanzeige rot und grün blinkt, gehen Sie wie folgt vor.

1. Überprüfen Sie die korrekte Konfiguration der Schalter.
2. Legen Sie die Sicherheitsnetzwerknummer fest.
3. Konfigurieren Sie das Gerät neu.

Beschreibung der DeviceNet-Netzwerkstatusanzeige (NS D)

Zustand der DeviceNet-Netzwerkstatusanzeige (NS D)	Bedeutung	Maßnahme
Aus	Die Steuerung ist nicht online oder wird über das DeviceNet-Netzwerk nicht mit Strom versorgt.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Grün, ein	Die Steuerung ist online; Verbindungen wurden hergestellt.	Keine Maßnahme erforderlich.
Grün, blinkend	Die Steuerung ist online; es wurden keine Verbindungen hergestellt.	
Rot, ein	Kommunikationsfehler aufgrund einer doppelten MAC-ID (Fehlercode F0) oder eines Busfehlers (Fehlercode F1).	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Rot, blinkend	Kommunikations-Timeout.	
Rot/Grün, blinkend	Die Sicherheitsnetzwerknummer (SNN) wird zurzeit eingestellt.	Keine Maßnahme erforderlich.

Wenn die Netzwerkstatusanzeige aus ist, gehen Sie wie folgt vor.

1. Schalten Sie die Stromversorgung aus und wieder ein.
2. Überprüfen Sie die externe Verdrahtung.
3. Überprüfen Sie, ob Störungen die Stromversorgung beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen.
4. Wenden Sie sich an Rockwell Automation.

Wenn Ihre Netzwerkstatusanzeige an ist oder rot blinkt, gehen Sie wie folgt vor.

1. Überprüfen Sie auf der alphanumerischen Anzeige den Fehlercode und die Netzknotenadresse des Fehlers.
2. Stellen Sie sicher, dass Netzknotenadressen nicht doppelt vergeben wurden.
3. Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden.
4. Vergewissern Sie sich, dass alle Kabel fest angeschlossen sind und die maximal zulässige Kabellänge nicht überschritten wird.
5. Vergewissern Sie sich, dass Abschlusswiderstände ausschließlich an beiden Enden der Hauptverbindung installiert wurden.
6. Überprüfen Sie, ob Störungen die Kommunikation beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen.
7. Stellen Sie sicher, dass die Zielgeräte konfiguriert und überprüft wurden und ordnungsgemäß funktionieren.

Beschreibung der Statusanzeige für Verriegelungskonfiguration (Lock)

Zustand der Anzeige für die Verriegelungskonfiguration (Lock)	Bedeutung	Maßnahme
Gelb, ein	Eine gültige, verriegelte Konfiguration ist vorhanden.	Keine Maßnahme erforderlich.
Gelb, blinkend	Eine gültige, nicht gesperrte Konfiguration ist vorhanden.	Sperren Sie die Konfiguration, bevor Sie das Sicherheitssystem in Betrieb nehmen.
Aus	Die Konfiguration ist ungültig.	Konfigurieren Sie die Steuerung neu.

Beschreibung der Statusanzeige für die USB-Konfiguration (Comm U)

Zustand der Anzeige für USB-Kommunikation (Comm U)	Bedeutung	Maßnahme
Gelb, blinkend	Die Steuerung führt zurzeit eine Kommunikation durch.	Keine Maßnahme erforderlich.
Aus	die Steuerung führt zurzeit keine Kommunikation durch.	

Beschreibung der E/A-Statusanzeige (Eingang 0 bis 15, Ausgang 0 bis 7)

Zustand der E/A-Statusanzeige	Bedeutung	Maßnahme
Rot, ein	Im Eingangs- oder Ausgangsschaltkreis wurde ein Fehler registriert oder es liegt ein Diskrepanzfehler im E/A-Satz für den Zweikanalmodus (Dual Channel Mode) vor.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Rot, blinkend	In der Zweikanalkonfiguration des zugehörigen E/A-Schaltkreises wurde ein Fehler registriert.	
Aus	Das Eingangs- oder Ausgangssignal ist ausgeschaltet.	
Gelb, ein	Das Eingangs- oder Ausgangssignal ist eingeschaltet.	Keine Maßnahme erforderlich.

Wenn Ihre E/A-Statusanzeige leuchtet oder rot blinkt, gehen Sie wie folgt vor.

1. Stellen Sie sicher, dass die Signalleitung:

- keinen Kontakt zur Stromquelle (positive Seite) hat.
- keinen Erdschluss aufweist.
- nicht getrennt wurde.

2. Vergewissern Sie sich, dass kein Kurzschluss zwischen den Signalleitungen vorliegt.

3. Stellen Sie sicher, dass am Ausgang kein Überstrom vorliegt.

4. Vergewissern Sie sich, dass kein Fehler in den angeschlossenen Geräten vorliegt.

5. Stellen Sie sicher, dass die Einstellungen für die Diskrepanzzeit (Discrepancy Time) gültig sind.

Wenn die E/A-Statusanzeige aus ist, gehen Sie wie folgt vor.

1. Vergewissern Sie sich, dass die eingestellte Spannung der Stromversorgung innerhalb des vorgeschriebenen Bereichs liegt.

2. Vergewissern Sie sich, dass alle Kabel- und Leitungsverbindungen einwandfrei sind.

Beschreibung der Statusanzeige für das EtherNet/IP-Netzwerk (NS E)

Zustand der EtherNet/IP-Statusanzeige (NS E)	Bedeutung	Maßnahme
Aus	Die Steuerung weist keine IP-Adresse auf oder ist nicht eingeschaltet.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Grün, blinkend	Die Steuerung verfügt über keine Verbindungen, jedoch über eine IP-Adresse.	
Grün, ein	Die Steuerung verfügt über mindestens eine Verbindung (z. B. zum Nachrichten-Router).	Keine Maßnahme erforderlich.
Rot, blinkend	Mindestens eine der Verbindungen, in denen dieses Gerät das Ziel ist, hat das Zeitlimit überschritten. Dieser Zustand darf nur unverändert bleiben, wenn alle Verbindungen mit Zeitlimitüberschreitung erneut hergestellt werden oder wenn das Gerät zurückgesetzt wird.	Die erforderliche Maßnahme finden Sie im Anschluss an diese Tabelle.
Rot, ein	Die Steuerung hat erkannt, dass ihre IP-Adresse bereits verwendet wird.	Setzen Sie die IP-Adresse zurück.

Wenn die EtherNet/IP-Statusanzeige aus ist, gehen Sie wie folgt vor.

1. Schalten Sie die Steuerung ein.
2. Legen Sie die IP-Adresse fest.

Wenn die EtherNet/IP-Statusanzeige grün blinkt, gehen Sie wie folgt vor.

1. Überprüfen Sie die Verdrahtung zur Steuerung.
2. Konfigurieren Sie den Master, sodass dieser eine Verbindung mit dem Ziel herstellt.

Wenn die EtherNet/IP-Statusanzeige rot blinkt, gehen Sie wie folgt vor.

1. Überprüfen Sie die externe Verdrahtung.
2. Überprüfen Sie die Endpunkte.
3. Überprüfen Sie die Schalter.

Beschreibung der Statusanzeige für die EtherNet/IP-Kommunikation (COMM E)

Zustand der Kommunikationsanzeige (COMM E)	Bedeutung	Maßnahme
Grün, ein	Die Steuerung kommuniziert im Ethernet-Netzwerk.	Keine Maßnahme erforderlich.
Aus	Die Steuerung kommuniziert nicht im Ethernet-Netzwerk.	

Beschreibung der Statusanzeige für die Ethernet-Netzwerkgeschwindigkeit (100)

Zustand der Anzeige für die Netzwerkgeschwindigkeit (100)	Bedeutung	Maßnahme
Gelb, ein	Die Kommunikationsgeschwindigkeit beträgt 100 Mbit/s.	Keine Maßnahme erforderlich.
Aus[1]	Die Kommunikationsgeschwindigkeit beträgt 10 Mbit/s.	Überprüfen Sie, ob die Anzeige für die Netzwerkgeschwindigkeit (10) leuchtet.

(1) Wenn diese Anzeige zusammen mit der Anzeige für die Netzwerkgeschwindigkeit (10) nicht leuchtet, überprüfen Sie Ihre Ethernet-Verbindung.

Beschreibung der Statusanzeige für die Ethernet-Netzwerkgeschwindigkeit (10)

Zustand der Anzeige für die Netzwerkgeschwindigkeit (10)	Bedeutung	Maßnahme
Gelb, ein	Die Kommunikationsgeschwindigkeit beträgt 10 Mbit/s.	Keine Maßnahme erforderlich.
Aus[1]	Die Kommunikationsgeschwindigkeit beträgt 100 Mbit/s.	Überprüfen Sie, ob die Anzeige für die Netzwerkgeschwindigkeit (100) leuchtet.

(1) Wenn diese Anzeige zusammen mit der Anzeige für die Netzwerkgeschwindigkeit (10) nicht leuchtet, überprüfen Sie Ihre Ethernet-Verbindung.

Fehleridentifikation mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige

In den folgenden Tabellen werden die verschiedenen Farb- und Zustandskombinationen der Status- und der alphanumerischen Anzeigen erläutert. Überprüfen Sie anhand der Tabellen, ob ggf. Korrekturmaßnahmen erforderlich sind.

Kritische Fehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**NS**	**Alphanumerische Anzeige, Code**			
Aus	Aus	Aus	Keine	Kritischer Hardware-Fehler. Störungspegel höher als erwartet.	1. Schalten Sie die Stromversorgung aus und wieder ein. 2. Überprüfen Sie die externe Verdrahtung. 3. Überprüfen Sie, ob Störungen die Stromversorgung beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen. 4. Wenden Sie sich an Rockwell Automation.
Rot, ein	Aus	Links: H Rechts: ---	System Failure (Systemfehler)	Kritischer Hardware-Fehler. Störungspegel höher als erwartet. Kurzschluss der Ausgangsklemme mit 24 V DC vor dem Betrieb.	
Rot, ein	Aus	P6	System Failure (Systemfehler)	Kurzschluss der Ausgangsklemme mit 24 V DC vor dem Betrieb.	1. Schalten Sie die Stromversorgung aus und wieder ein. 2. Überprüfen Sie die externe Verdrahtung.

Abbruchfehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**NS**	**Alphanumerische Anzeige[(1)], Code**			
Rot, blinkend	Grün, ein oder blinkend	E8	Switch setting mismatch (Fehlende Übereinstimmung der Schaltereinstellungen)	Netzknotenadresse und Baudrate wurden nach dem fehlerfreien Herunterladen der Konfiguration geändert.	1. Stellen Sie die Schalter richtig ein. 2. Konfigurieren Sie das Gerät neu.

(1) Die Anzeige zeigt abwechselnd den Fehlercode und die Netzknotenadresse des Fehlers an.

Nicht kritische Fehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**Alphanumerische Anzeige(1), Code**	**E/A**			
Rot, ein	F0	---	Duplicate MAC ID (Doppelte MAC-ID)	Für mehrere Netzknoten wurde dieselbe Netzknotenadresse eingestellt.	Stellen Sie sicher, dass keine Netzknotenadressen doppelt vergeben wurden, und konfigurieren Sie das Gerät bei Bedarf neu.
Rot, ein	F1	---	Bus Off (Bus unterbrochen)	Die Kommunikation wurde aufgrund häufiger Datenfehler unterbrochen.	1. Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. 2. Vergewissern Sie sich, dass alle Kabel fest angeschlossen sind und die maximal zulässige Kabellänge nicht überschritten wird. 3. Vergewissern Sie sich, dass Abschlusswiderstände ausschließlich an beiden Enden der Hauptverbindung installiert wurden. 4. Überprüfen Sie, ob Störungen die Kommunikation beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen. 5. Schalten Sie die Stromversorgung aus und wieder ein.
Rot, blinkend	L9	---	Standard I/O Connection Timeout (Timeout der Standard-E/A-Verbindung)	Es liegt ein Verbindungs-Timeout der Standard-E/A vor.	
Rot, blinkend	dA	---	Safety I/O Connection Timeout (Timeout der Sicherheits-E/A-Verbindung)	Es liegt ein Verbindungs-Timeout der Sicherheits-E/A vor.	
Rot, blinkend	d5	---	Nonexistent Slave Device (Slave-Gerät nicht vorhanden)	Es wurde kein Slave-Gerät gefunden.	
Rot, blinkend	d6	---	Safety I/O Connection Establishment Failure (Fehler beim Aufbau der Sicherheits-E/A-Verbindung)	Sicherheits-E/A-Verbindung konnte nicht hergestellt werden.	Stellen Sie sicher, dass das Slave-Gerät konfiguriert wurde und sich in einem normalen Betriebszustand befindet.
Rot, blinkend	d6	---	Invalid Slave Device (Ungültiges Slave-Gerät)	Ungültiges Slave-Gerät nach Überprüfungsfehler.	1. Überprüfen Sie die Konfiguration des Slave-Geräts. 2. Schließen Sie ein kompatibles Slave-Gerät an.
Aus	E0	---	Network PS Voltage Low (Versorgungsspannung des Netzwerks niedrig)	Die Versorgungsspannung des Netzwerks ist zu niedrig.	1. Stellen Sie sicher, dass die eingestellte Versorgungsspannung innerhalb des vorgeschriebenen Bereichs liegt. 2. Vergewissern Sie sich, dass alle Kabel und Leitungen fest angeschlossen sind.

Nicht kritische Fehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**Alphanumerische Anzeige[(1)], Code**	**E/A**			
---	E2	---	Transmission Timeout (Übertragungs-Timeout)	Timeout bei der DeviceNet-Übertragung oder kein Gerät an das DeviceNet-Netzwerk angeschlossen.	1. Stellen Sie sicher, dass alle Netzknoten dieselbe Kommunikationsgeschwindigkeit verwenden. 2. Vergewissern Sie sich, dass alle Kabel fest angeschlossen sind und die maximal zulässige Kabellänge nicht überschritten wird. 3. Vergewissern Sie sich, dass Abschlusswiderstände ausschließlich an beiden Enden der Hauptverbindung installiert wurden. 4. Überprüfen Sie, ob Störungen die Kommunikation beeinträchtigen und beseitigen Sie diese ggf. durch entsprechende Korrekturmaßnahmen.
Rot, blinkend	A0	---	Relevant Safety I/O communication stopped because of a Safety I/O communication error (Relevante Sicherheits-E/A-Kommunikation aufgrund eines Fehlers bei der Sicherheits-E/A-Kommunikation unterbrochen)	Bei einer Sicherheits-E/A-Verbindung ist ein Timeout aufgetreten. Die betreffende Sicherheits-E/A-Verbindung wurde deshalb unterbrochen.	
Rot, blinkend	A1	---	All Safety I/O communication stopped because of a Safety I/O communication error (Die gesamte Sicherheits-E/A-Kommunikation wurde aufgrund eines Fehlers bei der Sicherheits-E/A-Kommunikation unterbrochen)	Bei einer Sicherheits-E/A-Verbindung ist ein Timeout aufgetreten. Alle E/A-Verbindungen wurden deshalb unterbrochen.	
---	P4	Alle aus	Input PS Voltage Low (Eingangsspannungsversorgung niedrig)	Die E/A-Stromversorgung der Eingänge (V1, G1) ist nicht angeschlossen, obwohl eine Sicherheitseingangs- oder eine Testausgangsklemme verwendet wird.	1. Stellen Sie sicher, dass die eingestellte Versorgungsspannung innerhalb des vorgeschriebenen Bereichs liegt. 2. Vergewissern Sie sich, dass alle Kabel und Leitungen fest angeschlossen sind.
---	P5	Alle aus	Output PS Voltage Low (Ausgangsspannungsversorgung niedrig)	Die E/A-Stromversorgung der Ausgänge (V2, G2) ist nicht angeschlossen, obwohl eine Sicherheitsausgangsklemme verwendet wird.	

Nicht kritische Fehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**Alphanumerische Anzeige[(1)], Code**	**E/A**			
---	P1	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	External Test Signal Failure at Safety Input (Fehler des externen Testsignals am Sicherheitseingang)	An einem Sicherheitseingang wurde ein Fehler der externen Verdrahtung registriert.	1. Stellen Sie sicher, dass die Signalleitung: • keinen Kontakt zur Stromquelle (positive Seite) hat. • keinen Erdschluss aufweist. • nicht getrennt wurde. 2. Vergewissern Sie sich, dass kein Kurzschluss zwischen den Signalleitungen vorliegt. 3. Vergewissern Sie sich, dass kein Fehler in den angeschlossenen Geräten vorliegt. 4. Stellen Sie sicher, dass die Einstellungen für die Diskrepanzzeit gültig sind. Dieser Fehlerstatus wird gelöscht, wenn die Fehlerzeit für die Eingangsverriegelung abgelaufen und die Fehlerursache bis dahin behoben ist. Die Zielsicherheitseingänge müssen ausgeschaltet sein. Zum Ändern der Diskrepanzzeit müssen Sie den Sicherheitseingang neu konfigurieren.
---	P1	Zielklemme Rot, ein	Discrepancy Error at Safety Input (Diskrepanzfehler am Sicherheitseingang)	Zwischen zwei für den Zweikanalmodus konfigurierten Eingängen ist ein Diskrepanzfehler aufgetreten.	
---	P1	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	Internal Input Failure at Safety Input (Interner Eingangsfehler am Sicherheitseingang)	Am Sicherheitseingang wurde ein interner Schaltkreisfehler registriert.	
---	P2	Nicht anwendbar	Overload Detected at Test Output (Überlast am Testausgang festgestellt)	Bei einem als Standardsignalausgang konfigurierten Testausgang wurde eine Überlastung registriert.	Überprüfen Sie, ob das Ausgangsignal einen Erdschluss aufweist oder überlastet ist.
---	P2	Nicht anwendbar	Stuck-at-high Detected at Test Output (Blockierung im Ein-Zustand am Testausgang festgestellt)	Ein als Standardsignalausgang konfigurierter Testausgang ist im eingeschalteten Zustand blockiert.	1. Vergewissern Sie sich, dass die Stromversorgungsquelle (positive Seite) keinen Kontakt zur Ausgangssignalleitung hat. Schalten Sie den Eingang aus, sobald die Fehlerzeit für die Eingangsverriegelung abgelaufen ist und die Fehlerursache behoben wurde. Der Fehler wird zurückgesetzt. 2. Wenn kein Fehler bei der Verdrahtung vorliegt, tauschen Sie das Gerät aus.
---	P2	Nicht anwendbar	Undercurrent Detected Using Muting Lamp (Unterstrombedingung mittels Muting-Lampe festgestellt)	Am Testausgang wurde eine Trennung der Anzeigeleuchte registriert, während Klemme T3 als Signalausgang für die Muting-Lampe konfiguriert war.	1. Vergewissern Sie sich, dass die Verbindung des Ausgangssignalkabels einwandfrei ist. 2. Überprüfen Sie, ob die Anzeigeleuchte eventuell durchgebrannt ist.

Nicht kritische Fehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahmen
MS	**Alphanumerische Anzeige[(1)], Code**	**E/A**			
---	P3	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	Overcurrent Detected at Safety Output (Überstrom am Sicherheitsausgang festgestellt)	Am Sicherheitsausgang wurde ein Überstrom registriert.	1. Stellen Sie sicher, dass am Ausgang kein Überstrom vorliegt. 2. Stellen Sie sicher, dass die Signalleitung: • keinen Kontakt zur Stromquelle (positive Seite) hat. • keinen Erdschluss aufweist. 3. Vergewissern Sie sich, dass kein Kurzschluss zwischen den Signalleitungen vorliegt. Dieser Fehlerstatus wird gelöscht, wenn die Fehlerzeit für die Eingangsverriegelung abgelaufen und die Fehlerursache bis dahin behoben ist. Das Ausgangssignal der Benutzeranwendung für den Zielsicherheitsausgang muss ausgeschaltet werden.
---	P3	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	Short-circuit Detected at Safety Output (Kurzschluss am Sicherheitsausgang festgestellt)	Am Sicherheitsausgang wurde ein Kurzschluss festgestellt.	
---	P3	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	Stuck-at-high Detected at Safety Output (Blockierung im Ein-Zustand am Sicherheitsausgang festgestellt)	Ein Sicherheitsausgang ist im eingeschalteten Zustand blockiert.	
---	P3	Zielklemme Rot, ein Gepaarte Klemme Rot, blinkend	Cross Connection Detected at Safety Output (Querverbindung am Sicherheitsausgang festgestellt)	Am Sicherheitsausgang wurde eine Querverbindung registriert.	
---	P3	Zielklemme Rot, ein	Dual Channel Violation at Safety Output (Zweikanalfehler am Sicherheitsausgang)	Am Sicherheitsausgang wurde ein Ausgangsdatenfehler registriert. Dieser Fehler tritt z. B. auf, wenn ein Ausgang für den Zweikanalmodus konfiguriert wurde, aber nur eines der Ausgangsbits vom Programm eingeschaltet wird.	Stellen Sie sicher, dass die Programmausgangsdaten für zwei Ausgänge im Zweikanalmodus als gleichwertige Kanäle konfiguriert sind.

(1) Die Anzeige zeigt abwechselnd den Fehlercode und die Netzknotenadresse des Fehlers an.

Identifikation von EtherNet/IP-Fehlern mithilfe der Modulstatusanzeigen und der alphanumerischen Anzeige

In den folgenden Tabellen werden die verschiedenen Farb- und Zustandskombinationen der Status- und der alphanumerischen Anzeigen erläutert. Überprüfen Sie anhand der Tabellen, ob ggf. Korrekturmaßnahmen erforderlich sind.

Für die Steuerung 1752-L24BBBE zeigt die Anzeige die festgelegte EtherNet/IP-Adresse an, wenn der Schalter für die Anzeige der IP-Adresse mindestens 1 Sekunde lang gedrückt wird. Der Fehlercode „n4“ wird angezeigt, wenn in der EtherNet/IP-Konfiguration ein Fehler auftritt.

EtherNet/IP-Steuerungsfehler

Anzeigen			Fehlerprotokoll	Ursache	Erforderliche Maßnahme
MS	**NS**	**Alphanumerische Anzeige[(1)], Code**			
Aus	Rot, ein	UF	System Failure (Systemfehler)	Es ist ein Hardwarefehler des EtherNet/IP-Adapters aufgetreten.	Schalten Sie die Stromversorgung aus und wieder ein. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
Rot, ein	---	F0		Es ist ein IP-Adressverdopplungsfehler aufgetreten.	Überprüfen Sie die IP-Adressen der anderen Geräte und legen Sie eine Adresse fest, die noch nicht verwendet wird.
Aus	---	E3		Es ist ein Verbindungsfehler mit dem BOOTP-Server aufgetreten.	1. Stellen Sie sicher, dass das Kabel richtig angeschlossen ist. 2. Stellen Sie sicher, dass der BOOTP-Server normal arbeitet.
Aus	---	F2		Es ist ein Logikverarbeitungsfehler für die Basiseinstellung aufgetreten.	Überprüfen Sie die Konfiguration. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
Aus	Rot, blinkend	E9		Es ist ein EtherNet/IP-Speicherfehler aufgetreten.	Schalten Sie die Stromversorgung aus und wieder ein. Wenn erneut ein Fehler auftritt, ersetzen Sie die Steuerung.
Aus	Rot, blinkend	F4		Es ist ein Fehler der EtherNet/IP-Kommunikationssteuerung aufgetreten.	
Rot, blinkend	---	L9		Es ist ein Kommunikationsfehler des EtherNet/IP-Standardziels aufgetreten.	1. Stellen Sie sicher, dass dieselben Kommunikationseinstellungen für jeden Netzknoten verwendet werden. 2. Vergewissern Sie sich, dass die Kabel nicht abgezogen oder verbogen sind. 3. Stellen Sie sicher, dass der Master mit Strom versorgt wird.
Aus	---	E1		Es ist ein Fehler aufgrund einer unterbrochenen Verbindung aufgetreten.	1. Stellen Sie sicher, dass dieselben Kommunikationseinstellungen für jeden Netzknoten verwendet werden. 2. Vergewissern Sie sich, dass die Kabel nicht abgezogen oder verbogen sind. 3. Stellen Sie sicher, dass der Hub mit Strom versorgt wird.

(1) Die Anzeige zeigt abwechselnd den Fehlercode und „n4“ an.

Befehlsreferenz zu den Logikfunktionen

Einleitung

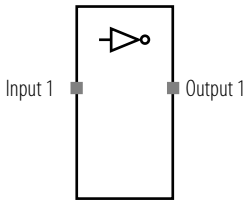
In diesem Anhang werden die für die Programmierung verwendeten Logikfunktionen beschrieben.

Thema	Seite
NOT-Befehl (Logisches Nicht)	219
AND-Befehl (Logisches Und)	220
OR-Befehl (Logisches Oder)	222
Exclusive OR-Befehl (Exklusives Oder)	224
Exclusive NOR-Befehl (Exklusives Nicht-Oder)	225
Routing-Befehl	226
RS-FF-Befehl (Reset Set Flip-flop)	226
Multi-connector-Befehl (Mehrere Anschlüsse)	227
Comparator-Befehl (Vergleicher)	228

NOT-Befehl (Logisches Nicht)

Das Ergebnis entspricht dem Kehrwert der Eingangs.

Diagramm NOT-Befehl



Wahrheitstabelle für den NOT-Befehl

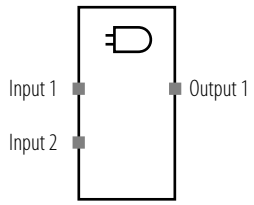
In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Input 1	Output 1
0	1
1	0

AND-Befehl (Logisches Und)

Der Ausgang entspricht einer logischen Und-Verknüpfung von bis zu acht Eingangsbedingungen. Die Anzahl der Eingänge kann im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Settings“ (E/A-Einstellungen) festgelegt werden. Die Standardeinstellung ist zwei Eingänge.

Diagramm AND-Befehl



Wahrheitstabelle für den AND-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN. Ein kleines x zeigt an, dass der Zustand nicht relevant ist.

Wahrheitstabelle für den AND-Befehl mit einem Eingang

Input 1	Output 1
0	0
1	1

Wahrheitstabelle für den AND-Befehl mit zwei Eingängen

Input 1	Input 2	Output 1
0	x	0
x	0	0
1	1	1

Wahrheitstabelle für den AND-Befehl mit drei Eingängen

Input 1	Input 2	Input 3	Output 1
0	x	x	0
x	0	x	0
x	x	0	0
1	1	1	1

Wahrheitstabelle für den AND-Befehl mit vier Eingängen

Input 1	Input 2	Input 3	Input 4	Output 1
0	x	x	x	0
x	0	x	x	0
x	x	0	x	0
x	x	x	0	0
1	1	1	1	1

Wahrheitstabelle für den AND-Befehl mit fünf Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Output 1
0	x	x	x	x	0
x	0	x	x	x	0
x	x	0	x	x	0
x	x	x	0	x	0
x	x	x	x	0	0
1	1	1	1	1	1

Wahrheitstabelle für den AND-Befehl mit sechs Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Output 1
0	x	x	x	x	x	0
x	0	x	x	x	x	0
x	x	0	x	x	x	0
x	x	x	0	x	x	0
x	x	x	x	0	x	0
x	x	x	x	x	0	0
1	1	1	1	1	1	1

Wahrheitstabelle für den AND-Befehl mit sieben Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Output 1
0	x	x	x	x	x	x	0
x	0	x	x	x	x	x	0
x	x	0	x	x	x	x	0
x	x	x	0	x	x	x	0
x	x	x	x	0	x	x	0
x	x	x	x	x	0	x	0
x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1

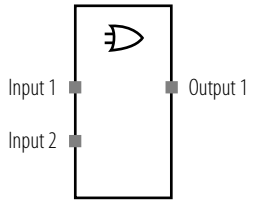
Wahrheitstabelle für den AND-Befehl mit acht Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Input 8	Output 1
0	x	x	x	x	x	x	x	0
x	0	x	x	x	x	x	x	0
x	x	0	x	x	x	x	x	0
x	x	x	0	x	x	x	x	0
x	x	x	x	0	x	x	x	0
x	x	x	x	x	0	x	x	0
x	x	x	x	x	x	0	x	0
x	x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1	1

OR-Befehl (Logisches Oder)

Der Ausgang entspricht einer logischen ODER-Verknüpfung von bis zu acht Eingangsbedingungen. Die Anzahl der Eingänge kann im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Settings“ (E/A-Einstellungen) festgelegt werden. Die Standardeinstellung ist zwei Eingänge.

Diagramm OR-Befehl



Wahrheitstabelle für den OR-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN. Ein kleines x zeigt an, dass der Zustand nicht relevant ist.

Wahrheitstabelle für den OR-Befehl mit einem Eingang

Input 1	Output 1
0	0
1	1

Wahrheitstabelle für den OR-Befehl mit zwei Eingängen

Input 1	Input 2	Output 1
0	0	0
1	x	1
x	1	1

Wahrheitstabelle für den OR-Befehl mit drei Eingängen

Input 1	Input 2	Input 3	Output 1
0	0	0	0
1	x	x	1
x	1	x	1
x	x	1	1

Wahrheitstabelle für den OR-Befehl mit vier Eingängen

Input 1	Input 2	Input 3	Input 4	Output 1
0	0	0	0	0
1	x	x	x	1
x	1	x	x	1
x	x	1	x	1
x	x	x	1	1

Wahrheitstabelle für den OR-Befehl mit fünf Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Output 1
0	0	0	0	0	0
1	x	x	x	x	1
x	1	x	x	x	1
x	x	1	x	x	1
x	x	x	1	x	1
x	x	x	x	1	1

Wahrheitstabelle für den OR-Befehl mit sechs Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Output 1
0	0	0	0	0	0	0
1	x	x	x	x	x	1
x	1	x	x	x	x	1
x	x	1	x	x	x	1
x	x	x	1	x	x	1
x	x	x	x	1	x	1
x	x	x	x	x	1	1

Wahrheitstabelle für den OR-Befehl mit sieben Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Output 1
0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	1
x	1	x	x	x	x	x	1
x	x	1	x	x	x	x	1
x	x	x	1	x	x	x	1
x	x	x	x	1	x	x	1
x	x	x	x	x	1	x	1
x	x	x	x	x	x	1	1

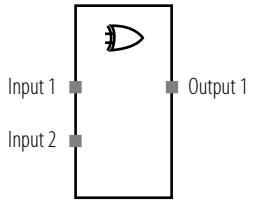
Wahrheitstabelle für den OR-Befehl mit acht Eingängen

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Input 8	Output 1
0	0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	x	1
x	1	x	x	x	x	x	x	1
x	x	1	x	x	x	x	x	1
x	x	x	1	x	x	x	x	1
x	x	x	x	1	x	x	x	1
x	x	x	x	x	1	x	x	x
x	x	x	x	x	x	1	x	1
x	x	x	x	x	x	x	1	1

Exclusive OR-Befehl (Exklusives Oder)

Das Ergebnis entspricht einer logischen, exklusiven Oder-Verknüpfung der Eingangsbedingungen.

Diagramm Exclusive OR-Befehl



Wahrheitstabelle für den Exclusive OR-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

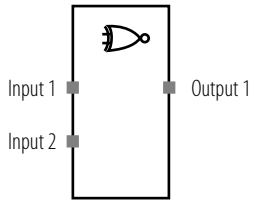
Wahrheitstabelle für die Exclusive OR-Bewertung

Input 1	Input 2	Output 1
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive NOR-Befehl (Exklusives Nicht-Oder)

Das Ergebnis entspricht einer logischen, exklusiven Nicht-Oder-Verknüpfung der Eingangsbedingungen.

Diagramm Exclusive NOR-Befehl



Wahrheitstabelle für den Exclusive NOR-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

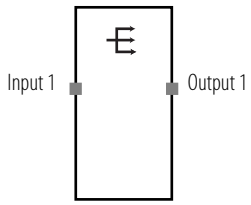
Wahrheitstabelle für die Exclusive NOR-Bewertung

Input 1	Input 2	Output 1
0	0	1
0	1	0
1	0	0
1	1	1

Routing-Befehl

Der Routing-Befehl leitet ein Eingangssignal an bis zu acht Ausgänge weiter. Er wird verwendet, um ein Signal an mehr als eine physische Adresse, z. B. ein Ausgangs-Tag, auszugeben. Die Anzahl der Ausgänge kann im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „I/O Setting“ (E/A-Einstellungen) festgelegt werden. Die Standardeinstellung ist 1.

Diagramm Routing-Befehl



Wahrheitstabelle für den Routing-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für die Routing-Bewertung

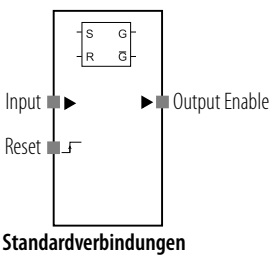
Input 1	Output 1	Output 2	Output 3	Output 4	Output 5	Output 6	Output 7	Output 8
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

RS-FF-Befehl (Reset Set Flip-flop)

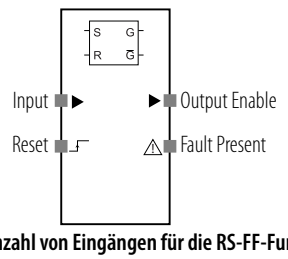
Durch Einschalten des Eingangssignals wird das Signal zur Aktivierung des Ausgangs „Output Enable“ eingeschaltet. „Output Enable“ bleibt auch beim Ausschalten des Eingangssignals eingeschaltet. Durch Einschalten des Reset-Signals wird das Signal „Output Enable“ ausgeschaltet.

Für die Programmierung kann auch der Ausgang „Fault Present“ verwendet werden. Um diesen optionalen Ausgang zu aktivieren, wählen Sie in der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „I/O Settings“ (E/A-Einstellungen) das Kontrollkästchen „Use Fault Present“ (Fault Present verwenden) aus.

Diagramm RS-FF-Befehl



Standardverbindungen



Maximale Anzahl von Eingängen für die RS-FF-Funktion

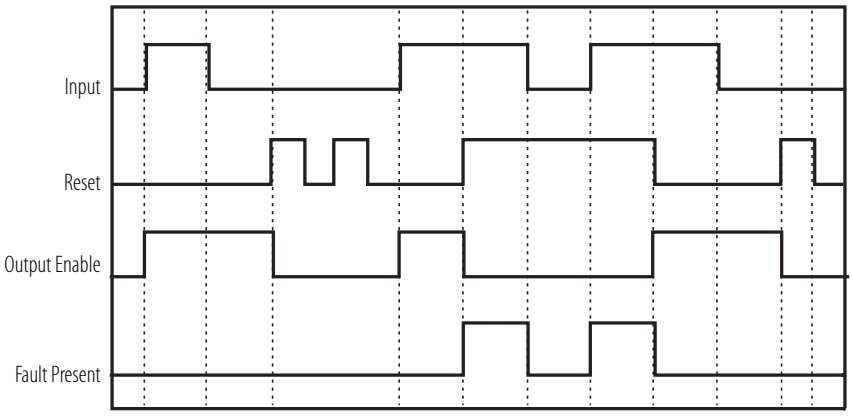
Fehlerhandhabung beim Reset Set Flip-flop-Befehl

Verwenden Sie diese Tabelle, um Diskrepanzfehler im RS-FF-Befehl zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen beim RS-FF-Befehl

Fehlerzustand	Zustand beim Auftreten des Fehlers		Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	
„Input" und „Reset" sind gleichzeitig aktiviert.	AUS (Sicherheitszustand)	EIN	Schalten Sie eines der Signale aus.

Zeitdiagramm für den RS-FF-Befehl

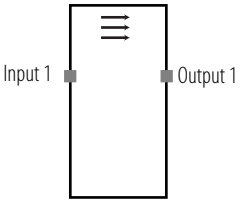


Multi-connector-Befehl (Mehrere Anschlüsse)

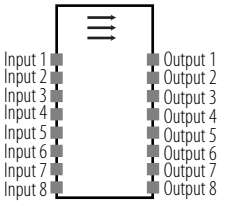
Der Multi-connector-Befehl konvertiert die Eingangssignale von bis zu acht Eingängen in Ausgangssignale für bis zu acht Ausgänge. Für die Eingangs- und Ausgangssignale eins bis acht gilt eine Eins-zu-Eins-Zuordnung. Der Zustand anderer Eingangssignale hat keinerlei Auswirkungen.

Die Anzahl der Ein- und Ausgänge kann in der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties" (Eigenschaften des Funktionsblocks) auf der Registerkarte „I/O Settings" (E/A-Einstellungen) bis auf acht erhöht werden. Die Standardeinstellung ist 1.

Diagramm Multi-connector-Befehl



Standardverbindungen



Maximale Anzahl von E/A für den Multi-connector-Befehl

Wahrheitstabelle für den Multi-connector-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

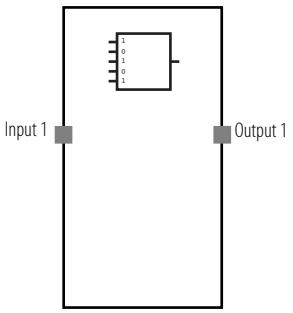
Wahrheitstabelle für den Multi-connector-Befehl

Eingänge								Ausgänge							
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x
1	x	x	x	x	x	x	x	1	x	x	x	x	x	x	x
x	0	x	x	x	x	x	x	x	0	x	x	x	x	x	x
x	1	x	x	x	x	x	x	x	1	x	x	x	x	x	x
x	x	0	x	x	x	x	x	x	x	0	x	x	x	x	x
x	x	1	x	x	x	x	x	x	x	1	x	x	x	x	x
x	x	x	0	x	x	x	x	x	x	x	0	x	x	x	x
x	x	x	1	x	x	x	x	x	x	x	1	x	x	x	x
x	x	x	x	0	x	x	x	x	x	x	x	0	x	x	x
x	x	x	x	1	x	x	x	x	x	x	x	1	x	x	x
x	x	x	x	x	0	x	x	x	x	x	x	x	0	x	x
x	x	x	x	x	1	x	x	x	x	x	x	x	1	x	x
x	x	x	x	x	x	0	x	x	x	x	x	x	x	0	x
x	x	x	x	x	x	1	x	x	x	x	x	x	x	1	x
x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	0
x	x	x	x	x	x	x	1	x	x	x	x	x	x	x	1

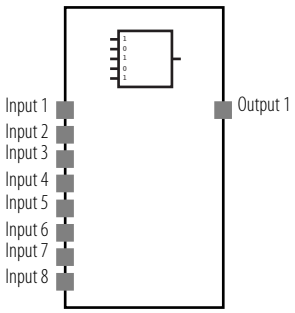
Comparator-Befehl (Vergleicher)

Der Comparator-Befehl vergleicht die angegebenen Eingangssignale von bis zu acht Eingängen mit dem konfigurierten Vergleichsmuster und schaltet „Output 1“ ein, wenn alle Eingangssignale dem Vergleichsmuster entsprechen. „Output 1“ wird ausgeschaltet, sobald die Eingangssignale nicht mehr mit dem Vergleichswert übereinstimmen.

Diagramm Comparator-Befehl



Standardverbindungen



Maximale Anzahl von E/A für den Comparator-Befehl

Parameter des Comparator-Befehls

Stellen Sie diese Parameter für den Comparator-Befehl ein.

Parameter des Comparator-Funktionsblocks

Parameter	Gültiger Bereich	Standardeinstellung
Vergleichswert	00000000…11111111 (Bit 7…0)	00000001

Sie können das Vergleichsmuster und die Anzahl der Eingänge (bis zu acht) in der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Setting“ (E/A-Einstellungen) einstellen. In der Standardeinstellung ist ein Eingang konfiguriert. Verwenden Sie für das Vergleichsmuster eine Kombination der Werte 0 (Eingang aus), 1 (Eingang ein) und X (Eingang ein oder aus).

Wahrheitstabelle für den Comparator-Befehl

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN. CV bezeichnet den Vergleichswert (Comparison Value). Ein X zeigt an, dass der Zustand des Eingangs (Übereinstimmung oder keine Übereinstimmung) keinen weiteren Einfluss auf das Ergebnis hat.

Wahrheitstabelle für den Comparator-Befehl

Input 8	Input 7	Input 6	Input 5	Input 4	Input 3	Input 2	Input 1	Output 1
≠CV für Bit 7	X	X	X	X	X	X	X	0
X	≠CV für Bit 6	X	X	X	X	X	X	0
X	X	≠CV für Bit 5	X	X	X	X	X	0
X	X	X	≠CV für Bit 4	X	X	X	X	0
X	X	X	X	≠CV für Bit 3	X	X	X	0
X	X	X	X	X	≠CV für Bit 2	X	X	0
X	X	X	X	X	X	≠CV für Bit 1	X	0
X	X	X	X	X	X	X	≠CV für Bit 0	0
= CV für Bit 7	= CV für Bit 6	= CV für Bit 5	= CV für Bit 4	= CV für Bit 3	= CV für Bit 2	= CV für Bit 1	= CV für Bit 0	1

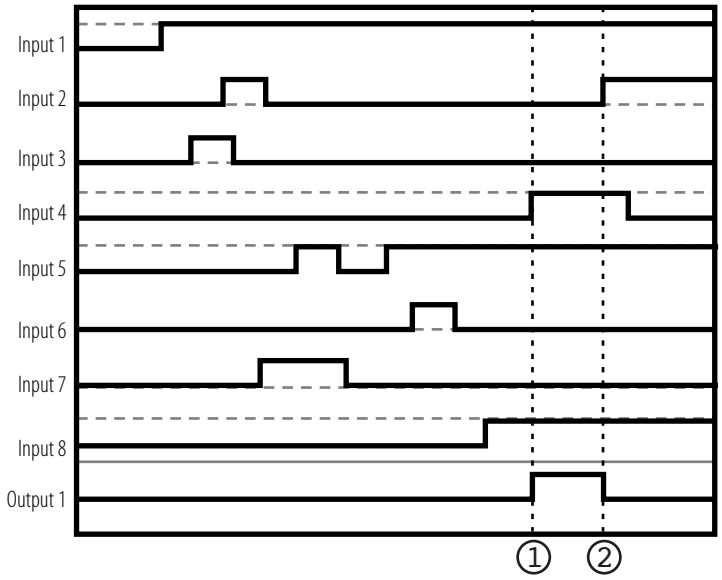
Zeitdiagramm für den Comparator-Befehl

Die horizontalen gestrichelten Linien im Diagramm stellen die Vergleichswerte (CV) der Eingänge dar.

1. „Output 1“ wird eingeschaltet, sobald alle Eingangssignale mit dem Vergleichswert übereinstimmen.

2. „Output 1“ wird ausgeschaltet, sobald eines der Eingangssignale nicht mit dem Vergleichswert übereinstimmt.

Zeitdiagramm für den Comparator-Befehl



Notizen:

Befehlsreferenz zu den Funktionsblöcken

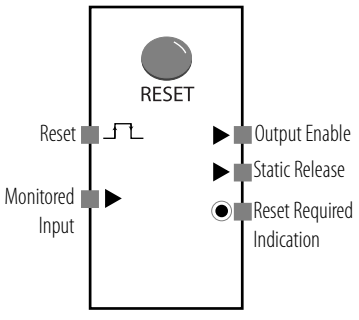
Einleitung

In diesem Anhang werden die für die Programmierung verwendeten Funktionsblöcke beschrieben.

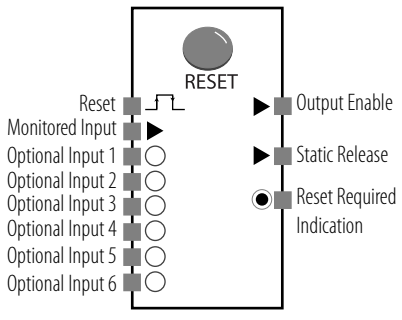
Thema	Seite
Funktionsblock Reset (Zurücksetzen)	233
Funktionsblock „Restart" (Neustart)	235
Not-Aus (ESTOP)	237
Funktionsblock „Light Curtain" (Lichtgitter) (LC)	240
Funktionsblock „Safety Gate Monitoring" (Sicherheitstürüberwachung)	242
Funktionsblock Two-hand Control (2-Hand-Betätigung)	247
Funktionsblock OFF-delay Timer (Ausschaltverzögerter Timer)	251
Funktionsblock „ON-delay Timer" (Einschaltverzögerter Timer)	251
Funktionsblock „User Mode Switch" (Anwendermodus-Schalter)	252
External Device Monitoring (EDM, Externe Geräteüberwachung)	254
Muting	256
Enable Switch (Zustimmschalter)	273
Pulse Generator (Impulsgenerator)	276
Counter (Zähler)	277

Funktionsblock Reset (Zurücksetzen)

Diagramm des Funktionsblocks Reset



Standardverbindungen



Maximale Anzahl von Eingängen für die Reset-Funktion

In der Software RSNetWorx for DeviceNet kann die Anzahl der Eingänge im Dialogfeld „Function Block Properties" (Eigenschaften des Funktionsblocks) auf der Registerkarte „I/O Settings" (E/A-Einstellungen) von zwei auf acht erhöht werden. In der Standardeinstellung werden zwei Eingänge verwendet.

Das Signal „Output Enable“ (Ausgangsaktivierung) wird aktiviert, wenn das Signal „Reset“ korrekt empfangen wurde, während die Bedingung „Monitored Input“ (Überwachter Eingang) am Reset-Funktionsblock aktiviert ist. Mit diesem Funktionsblock kann ein automatischer Reset der Maschine beim Einschalten der Stromversorgung der Steuerung, beim Wechsel aus dem Betriebsmodus Idle (Leerlauf) in den Run-Modus (Betrieb) oder beim Einschalten eines Gerätesignals auf einem Sicherheitseingang verhindert werden.

„Static Release“ (Statisches Signal Freigabe Bedingung erfüllt) und „Reset Required Indication“ (Reset erforderlich-Anzeige) sind optionale Ausgänge. Um einen dieser Ausgänge zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) das entsprechende Kontrollkästchen auf der Registerkarte „Out point“ (Ausgangspunkt) aus.

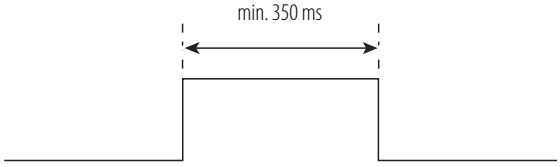
Bedingungen für das Einschalten eines Ausgangs

Ausgang	Einschaltbedingung
Output Enable	„Monitored Input“ (Überwachter Eingang) und alle aktivierten optionalen Eingänge müssen eingeschaltet sein, und das Reset-Signal muss ordnungsgemäß empfangen werden.
Static Release	„Monitored Input“ und alle aktivierten optionalen Eingänge müssen eingeschaltet sein.
Reset Required Indication	Auf „Reset Required Indication“ (Anzeige Reset erforderlich) wird ein 1-Hz-Impuls ausgegeben, wenn „Monitored Input“ und alle aktivierten optionalen Eingänge eingeschaltet sind und das Signal „Output Enable“ ausgeschaltet ist. „Reset Required Indication“ wird nur eingeschaltet, wenn das Reset-Signal eingeschaltet ist.

Parameter des Funktionsblocks Reset

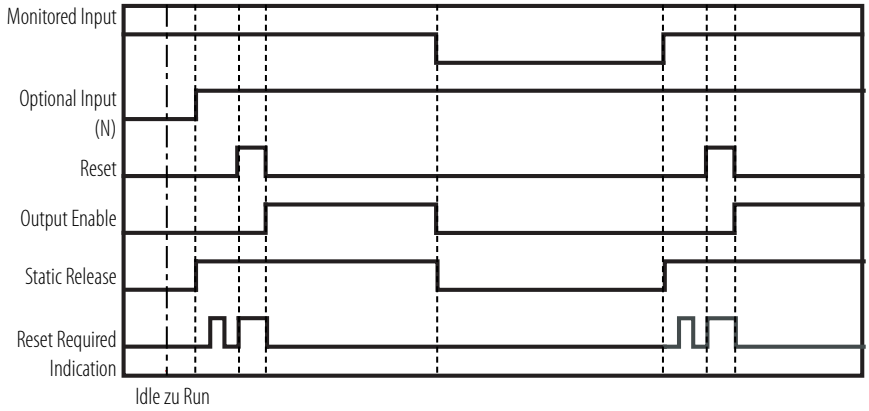
Im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Parameter“ können Sie das Reset-Signal entweder auf „Low-High-Low“ (Niedrig-Hoch-Niedrig) oder auf „Rising Edge“ (Steigende Flanke) einstellen. Die Standardeinstellung ist „Low-High-Low“.

Bei einer Konfiguration für „Low-High-Low“ muss das Reset-Signal die folgenden Vorgaben erfüllen.

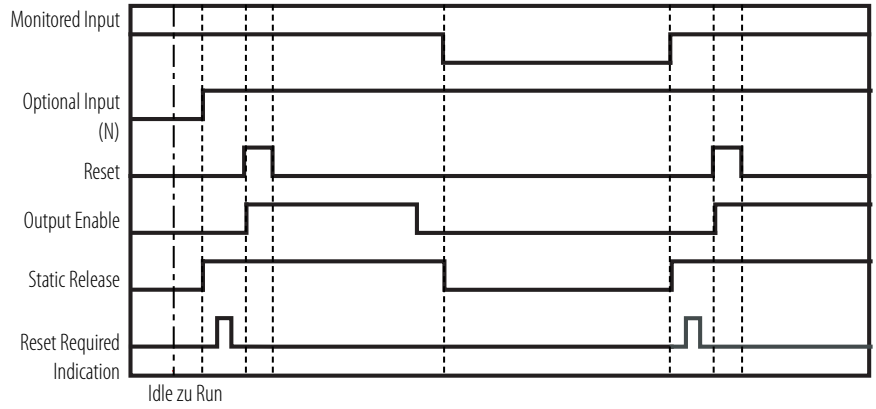


Zeitdiagramme für den Funktionsblock Reset

Reset-Signal „Low-High-Low" (Niedrig-Hoch-Niedrig)

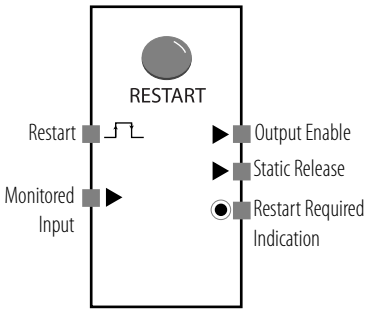


Reset-Signal „Rising Edge" (Steigende Flanke)

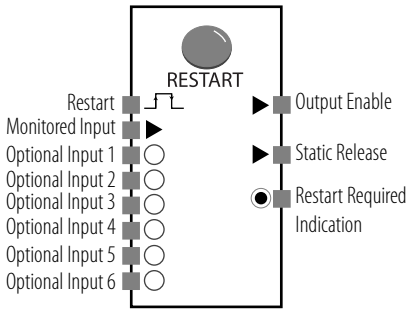


Funktionsblock „Restart" (Neustart)

Diagramm des Funktionsblocks „Restart" (Neustart)



Standardverbindungen



Maximale Anzahl von Eingängen für die Restart-Funktion

In der Software RSNetWorx for DeviceNet kann die Anzahl der Eingänge im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „I/O Settings“ (E/A-Einstellungen) von zwei auf acht erhöht werden. In der Standardeinstellung werden zwei Eingänge verwendet.

Das Signal „Output Enable“ (Ausgangsaktivierung) wird aktiviert, wenn das Signal „Restart“ (Neustart) ordnungsgemäß empfangen wird, während die Bedingung „Monitored Input“ (Überwachter Eingang) am Restart-Funktionsblock anliegt. Mit diesem Funktionsblock kann ein automatischer Neustart der Maschine beim Einschalten der Stromversorgung der Steuerung, beim Wechsel des Betriebsmodus oder beim Einschalten eines Gerätesignals auf einem Sicherheitseingang verhindert werden. Reset und Restart sind in ihrer Funktion identisch.

„Static Release“ (Statisches Signal Freigabe Bedingung erfüllt) und „Restart Required Indication“ (Neustart erforderlich-Anzeige) sind optionale Ausgänge. Um einen dieser Ausgänge zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) das entsprechende Kontrollkästchen auf der Registerkarte „Out point“ (Ausgangspunkt) aus.

Bedingungen für das Einschalten eines Ausgangs

Ausgang	Einschaltbedingung
Output Enable	„Monitored Input“ (Überwachter Eingang) und alle aktivierten optionalen Eingänge müssen eingeschaltet sein und es muss ein Restart-Signal ordnungsgemäß empfangen werden.
Static Release	„Monitored Input“ und alle aktivierten optionalen Eingänge müssen eingeschaltet sein.
Restart Required Indication	Auf „Restart Required Indication“ (Anzeige Neustart erforderlich) wird ein 1-Hz-Impuls ausgegeben, wenn „Monitored Input“ und alle aktivierten optionalen Eingänge eingeschaltet sind und das Signal „Output Enable“ ausgeschaltet ist. „Restart Required Indication“ wird nur eingeschaltet, wenn das Restart-Signal eingeschaltet ist.

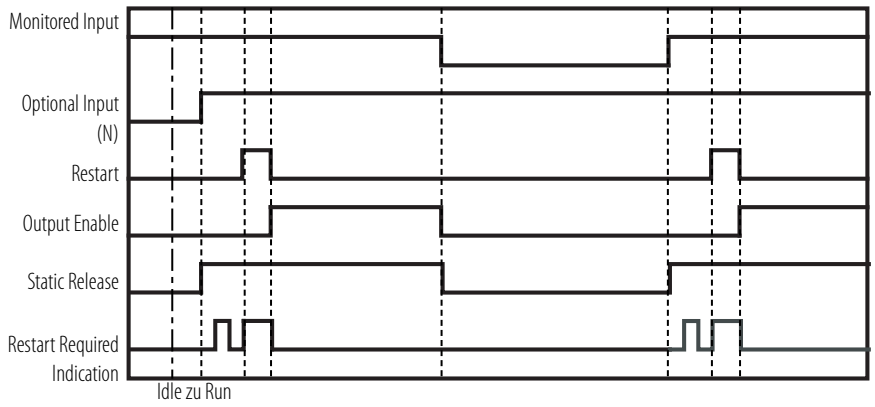
Parameter des Funktionsblocks Restart

Im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Parameter“ können Sie das Restart-Signal entweder auf „Low-High-Low“ (Niedrig-Hoch-Niedrig) oder auf „Rising Edge“ (Steigende Flanke) einstellen. Die Standardeinstellung ist „Low-High-Low“.

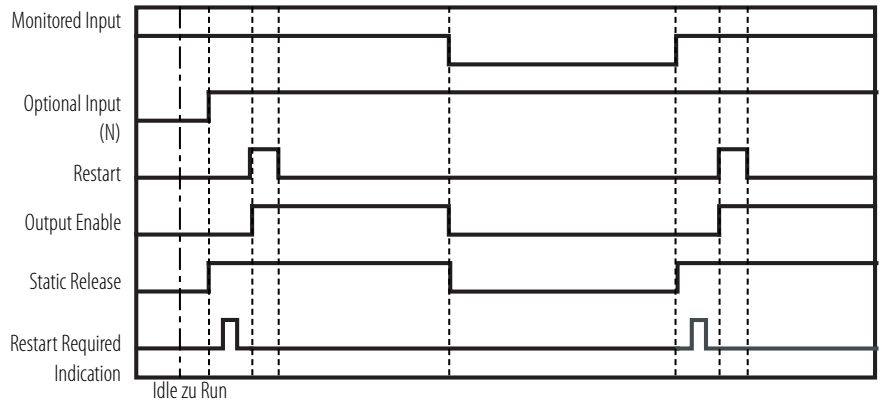
Bei einer Konfiguration für „Low-High-Low“ muss das Restart-Signal die folgenden Vorgaben erfüllen.

Zeitdiagramme für den Funktionsblock „Restart“ (Neustart)

Restart-Signal „Low-High-Low“ (Niedrig-Hoch-Niedrig)

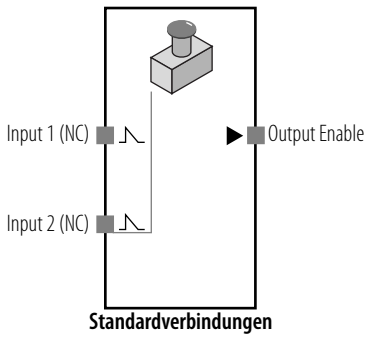


Restart-Signal „Rising Edge“ (Steigende Flanke)

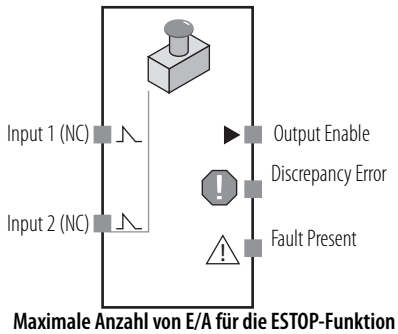


Not-Aus (ESTOP)

Diagramm des Funktionsblocks „ESTOP“



Standardverbindungen



Maximale Anzahl von E/A für die ESTOP-Funktion

Mit der Überwachungsfunktion für den Not-Aus-Taster können Sie einen Not-Aus-Schalter überwachen. Das Signal „Output Enable“ (Ausgangsaktivierung) wird eingeschaltet, sobald die mit dem überwachten Notschalter verbundenen Eingänge aktiv sind. „Output Enable“ wird ausgeschaltet, wenn die Eingänge inaktiv werden oder wenn für den Funktionsblock ein Fehler registriert wird.

WICHTIG Für Not-Aus-Anwendungen ist eine manuelle Reset-Funktion erforderlich. Wenn Sie den Funktionsblock für Not-Aus-Schalter verwenden, müssen Sie auch den Reset-Funktionsblock verwenden.

Der Ausgang „Discrepancy Error“ (Diskrepanzfehler) kann während der Programmierung des ESTOP-Funktionsblocks verwendet werden. Um diesen optionalen Ausgang anzuzeigen, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Discrepancy Error“ (Diskrepanzfehler).

Für die Programmierung kann auch der Ausgang „Fault Present“ verwendet werden. Um diesen optionalen Ausgang zu aktivieren, aktivieren Sie im Dialogfeld „Function Block Properties“ auf der Registerkarte „Out point“ das Kontrollkästchen „Fault Present“.

Parameter des Funktionsblocks „ESTOP“

Stellen Sie diese Parameter für den Funktionsblock ESTOP ein.

Parameter des Funktionsblocks „ESTOP“

Parameter	Gültiger Bereich	Standardeinstellung
Input Type (Eingangstyp)	Einkanal, Zweikanal-Äquivalent Zweikanal-Komplement	Zweikanal-Äquivalent
Discrepancy Time (Diskrepanzzeit)	0 bis 30 s in Schritten von 10 ms.(1) Die Diskrepanzzeit muss gleich oder größer als die Zykluszeit der Steuerung sein.	30 ms

(1) Wenn die Diskrepanzzeit auf 0 eingestellt wird, erfolgt keine Überprüfung.

Wahrheitstabelle für den Funktionsblock „ESTOP“

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für den Funktionsblock „ESTOP“

Einkanal		Zweikanal-Äquivalent			Zweikanal-Komplement		
Input 1 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable	Input 1 (NC)	Input 2 (NO)	Output Enable
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Fehlerbehandlung für den Funktionsblock „ESTOP“

Es wird ein Diskrepanzfehler generiert, wenn sich einer der Eingänge länger als durch die Diskrepanzzeit angegeben in einem nicht korrekten Zustand befindet. Im Modus Zweikanal-Äquivalent müssen beide Eingänge beispielsweise innerhalb der Diskrepanzzeit aktiv (eingeschaltet) sein. Andernfalls wird ein Fehler ausgegeben.

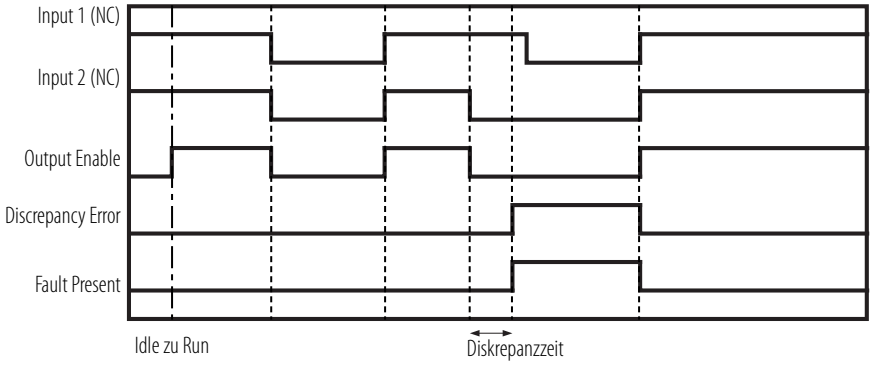
Verwenden Sie diese Tabelle, um Diskrepanzfehler im ESTOP-Funktionsblock zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks „ESTOP“

Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehler-ausgang	
Discrepancy Error (Diskre-panzfehler)	AUS (Sicherheitszustand)	EIN	Ausgang „Discrepancy Error“: EIN	Beseitigen Sie die Ursache für den Fehler und: 1. Schalten Sie die Eingänge ein und wieder aus. 2. Schalten Sie die Steuerung in den Betriebsmodus „Idle“ (Leerlauf) und wieder zurück nach „Run“ (Betrieb).

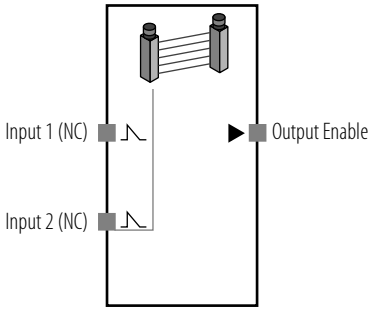
Zeitdiagramm für den Funktionsblock „ESTOP“

In diesem Diagramm sind die E/A-Zeiten für die Konfiguration des Funktionsblocks im Modus Zweikanal-Äquivalent dargestellt.

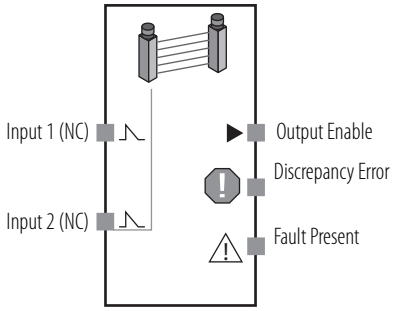


Funktionsblock „Light Curtain“ (Lichtgitter) (LC)

Diagramm des Funktionsblocks „Light Curtain“ (Lichtgitter)



Standardverbindungen



Maximale Anzahl von E/A für die Light Curtain-Funktion

Der Überwachungsfunktionsblock Light Curtain (LC) überwacht ein Typ-4-Sicherheitslichtgitter. Das Signal „Output Enable“ wird eingeschaltet, sobald die mit dem überwachten Sicherheitslichtgitter verbundenen Eingänge aktiv sind. Das Signal „Output Enable“ wird ausgeschaltet, wenn die Eingänge inaktiv werden oder wenn für den Funktionsblock ein Fehler registriert wird.

Sie können den Ausgang „Discrepancy Error“ während der Programmierung des LC-Funktionsblocks verwenden. Um diesen optionalen Diagnoseausgang anzuzeigen, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Discrepancy Error“ (Diskrepanzfehler).

Für die Programmierung kann auch der Ausgang „Fault Present“ verwendet werden. Um diese optionalen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Fault Present“ (Fehler vorhanden) aus.

Parameter des Funktionsblocks „Light Curtain“ (Lichtgitter)

Stellen Sie diese Parameter für den LC-Funktionsblock ein.

Parameter des LC-Funktionsblocks

Parameter	Gültiger Bereich	Standardeinstellung
Input Type (Eingangstyp)	Zweikanal-Äquivalent Zweikanal-Komplement	Zweikanal-Äquivalent
Discrepancy Time (Diskrepanzzeit)	0 bis 30 s in Schritten von 10 ms.(1) Die Diskrepanzzeit muss gleich oder größer als die Zykluszeit der Steuerung sein.	30 ms

(1) Wenn die Diskrepanzzeit auf 0 eingestellt wird, erfolgt keine Überprüfung.

Wahrheitstabellen für den Funktionsblock „Light Curtain“ (Lichtgitter)

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für den LC-Funktionsblock

Zweikanal-Äquivalent			Zweikanal-Komplement		
Input 1 (NC)	**Input 2 (NC)**	**Output Enable**	**Input 1 (NC)**	**Input 2 (NC)**	**Output Enable**
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	1
1	1	1	1	1	0

Fehlerbehandlung für den Funktionsblock „Light Curtain“ (Lichtgitter)

Es wird ein Diskrepanzfehler generiert, wenn sich einer der Eingänge länger als durch die Diskrepanzzeit angegeben in einem nicht korrekten Zustand befindet. Im Modus Zweikanal-Äquivalent müssen beide Eingänge beispielsweise innerhalb der Diskrepanzzeit aktiv (eingeschaltet) sein. Andernfalls wird ein Fehler ausgegeben.

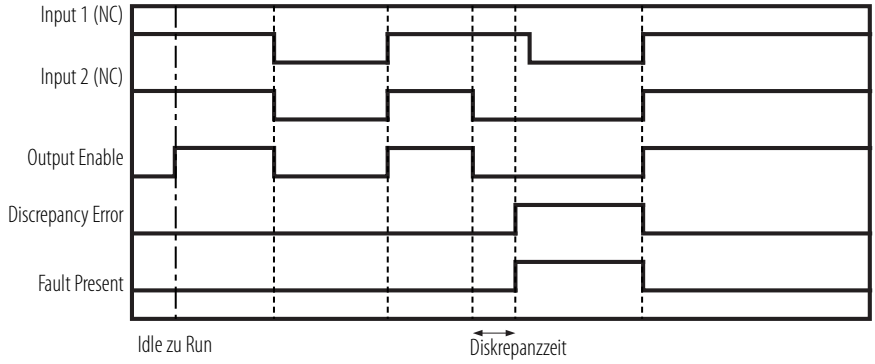
Verwenden Sie diese Tabelle, um Diskrepanzfehler im LC-Funktionsblock zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des LC-Funktionsblocks

Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehler-ausgang	
Discrepancy Error (Diskrepanz-fehler)	AUS (Sicherheitszustand)	EIN	Ausgang „Discrepancy Error“: EIN	Beseitigen Sie die Ursache für den Fehler und: 1. Schalten Sie die Eingänge aus und wieder ein. 2. Schalten Sie die Steuerung in den Betriebsmodus „Idle“ (Leerlauf) und wieder zurück nach „Run“ (Betrieb).

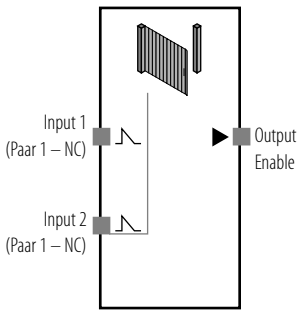
Zeitdiagramm für den Funktionsblock „Light Curtain“ (Lichtgitter)

In diesem Diagramm sind die E/A-Zeiten für die Konfiguration des Funktionsblocks im Modus Zweikanal-Äquivalent dargestellt.

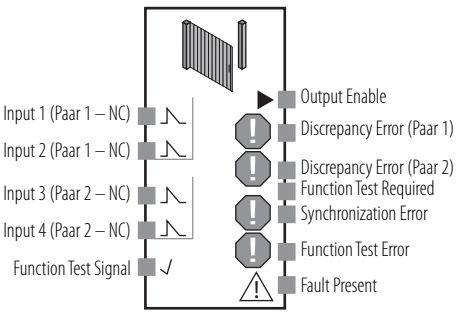


Funktionsblock „Safety Gate Monitoring“ (Sicherheitstürüberwachung)

Diagramm des Funktionsblocks „Safety Gate Monitoring“ (Sicherheitstürüberwachung)



Standardverbindungen



Maximale Anzahl von E/A für die Safety Gate-Funktion

Die Safety Gate Monitoring-Funktion überwacht den Status einer Sicherheitstür anhand der Eingangssignale eines mit der Tür verbundenen Sicherheitstürschalters oder Sicherheits-Endschalters. Das Signal „Output Enable“ (Ausgangsaktivierung) wird eingeschaltet, sobald die mit dem überwachten Schalter verbundenen Eingänge aktiv sind. Das Signal „Output Enable“ wird ausgeschaltet, wenn die Eingänge inaktiv werden oder wenn für diesen Funktionsblock ein Fehler registriert wird.

Optionale Ausgänge für den Funktionsblock „Safety Gate Monitoring“ (Sicherheitstürüberwachung)

Die optionalen Ausgänge können auch für die Programmierung verwendet werden. Um diese optionalen Ausgänge anzuzeigen, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das entsprechende Kontrollkästchen.

- Discrepancy Error Pair 1
- Discrepancy Error Pair 2
- Function Test Required Signal
- Sychronization Error
- Function Test Error

Einstellung des Ausgangs „Fault Present“ für den Funktionsblock „Safety Gate Monitoring“

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Fault Present“ aus.

Funktionstests für den Funktionsblock „Safety Gate Monitoring“

Bei einigen Sicherheitstüranwendungen (z. B. Kategorie 2) wird für Sicherheitsgeräte vorgeschrieben, dass eine physische Überprüfung der ordnungsgemäßen Türfunktion erfolgt.

Wenn der Funktionstest für den Safety Gate Monitoring-Funktionsblock aktiviert ist, kann ein Test der Sicherheitstür, bei dem die Sicherheitstür physisch geöffnet und wieder geschlossen wird, als Bedingung für das Einschalten des Signals „Output Enable“ (Ausgangsaktivierung) hinzugefügt werden.

Bei Aktivierung muss der Sicherheitstürtest unter Berücksichtigung der folgenden Bedingungen durchgeführt werden:

- Start – Der Test der Sicherheitstür muss beim Einschalten der Steuerung durchgeführt werden, d. h., sobald die Steuerung aus dem Modus „Idle“ (Leerlauf) in den Modus „Run“ (Betrieb) wechselt. Wenn der Test normal abgeschlossen wird, führt dies zum Einschalten der Signals „Output Enable“ (Ausgangsaktivierung).
- Funktionstestanforderung der Maschine – Der Test der Sicherheitstür muss durchgeführt werden, nachdem die Steuerung das Funktionstestsignal von der Maschine registriert hat und dieses eingeschaltet wird, jedoch noch bevor das Funktionstestsignal erneut eingeschaltet wird. Wenn das Funktionstestsignal vor dem normalen Abschluss des Sicherheitstürtests ein zweites Mal eingeschaltet wird, führt dies zu einem Funktionstestfehler: das Signal „Output Enable“ (Ausgangsaktivierung) wird ausgeschaltet, und das Funktionstestfehler-Signal wird eingeschaltet.
- Registrierter Fehler im Funktionsblock Safety Gate Monitoring – Wenn ein Funktionstestfehler, ein Diskrepanzfehler oder ein anderer Funktionsblockfehler auftritt, muss nach dem Beheben der Fehlerursache ein Sicherheitstürtest durchgeführt werden.

Das Signal „Function Test Required“ (Funktionstest erforderlich) des Funktionsblocks Safety Gate Monitoring wird eingeschaltet, sobald ein Test der Sicherheitstür erforderlich ist. Das Signal bleibt eingeschaltet, bis der Sicherheitstürtest normal abgeschlossen wurde.

Parameter des Funktionsblocks „Safety Gate Monitoring“

Stellen Sie diese Parameter für den Funktionsblock Safety Gate Monitoring ein.

Parameter des Funktionsblocks „Safety Gate Monitoring“

Parameter	Bereich	Standard
Input Type (Eingangstyp)	Einkanal Zweikanal-Äquivalent (1 Paar) Zweikanal-Komplement (1 Paar) Zwei Zweikanal-Äquivalent (2 Paare) Zwei Zweikanal-Komplement (2 Paare)	Zweikanal-Äquivalent
Function Test (Funktionstest)	Kein Funktionstest/Funktionstest erforderlich	Kein Funktionstest
Discrepancy Time Pair 1 (Diskrepanzzeit Paar 1)	0 bis 30 s in Schritten von 10 ms Beim Wert 0 wird keine Prüfung der Synchronisationszeit durchgeführt.	30 ms
Discrepancy Time Pair 2 (Diskrepanzzeit Paar 2)		
Synchronization Time (Synchronisationszeit)	0 bis 30 s in Schritten von 10 ms Beim Wert 0 wird keine Prüfung der Synchronisationszeit durchgeführt.	300 ms

Wahrheitstabellen für den Funktionsblock „Safety Gate Monitoring“

In den Booleschen Tabellen steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für den Funktionsblock „Safety Gate Monitoring“, Einkanal und Zweikanal (1 Paar)

Einkanal		Zweikanal-Äquivalent			Zweikanal-Komplement		
Input 1 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Wahrheitstabelle für den Funktionsblock „Safety Gate Monitoring“, Zweikanal (2 Paare)

Zweikanal-Äquivalent (2 Paare)					Zweikanal-Komplement (2 Paare)				
Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	1	0	0
0	0	1	1	0	0	0	1	1	0
0	1	0	0	0	0	1	0	0	0
0	1	0	1	0	0	1	0	1	0
0	1	1	0	0	0	1	1	0	0
0	1	1	1	0	0	1	1	1	0
1	0	0	0	0	1	0	0	0	0
1	0	0	1	0	1	0	0	1	0
1	0	1	0	0	1	0	1	0	1
1	0	1	1	0	1	0	1	1	0
1	1	0	0	0	1	1	0	0	0
1	1	0	1	0	1	1	0	1	0
1	1	1	0	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	0

Fehlerbehandlung für den Funktionsblock „Safety Gate Monitoring“

Es wird ein Diskrepanzfehler generiert, wenn sich einer der Eingänge länger als durch die Diskrepanzzeit angegeben in einem nicht korrekten Zustand befindet. Im Modus Zweikanal-Äquivalent müssen beide Eingänge beispielsweise innerhalb der Diskrepanzzeit aktiv (eingeschaltet) sein. Andernfalls wird ein Fehler ausgegeben.

Wenn zwei Eingangspaare ausgewählt sind und eine Synchronisationszeit eingegeben wurde, müssen beide Eingangspaare innerhalb der Synchronisationszeit denselben Zustand aufweisen. Andernfalls wird ein Synchronisationsfehler ausgegeben. Die Diskrepanzzeit regelt die Zustandsübereinstimmung für beide Eingänge eines Eingangspaares innerhalb der angegebenen Zeit, während die Synchronisationszeit die Übereinstimmung beider Eingangspaare innerhalb der angegebenen Zeit regelt.

Verwenden Sie diese Tabelle, um Diskrepanzfehler im Funktionsblock Safety Gate Monitoring zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks „Safety Gate Monitoring“

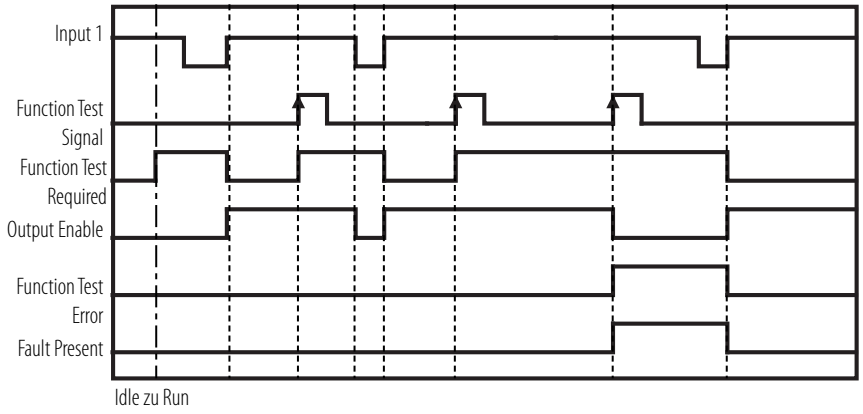
Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands	
	Output Enable	Fault Present	Fehlerausgang	Bei deaktiviertem Funktionstest	Bei aktiviertem Funktionstest
Diskrepanzfehler auf Paar 1	AUS (Sicherheitszustand)	EIN	Discrepancy Error Pair 1: EIN	Beseitigen Sie die Ursache für den Fehler und 1. Schalten Sie die Eingänge ein und wieder aus.(2) 2. Schalten Sie die Steuerung in den Betriebsmodus „IDLE“ (Leerlauf) und wieder zurück nach „RUN“ (Betrieb).	Beheben Sie die Fehlerursache, und schalten Sie dann die Eingänge ein und wieder aus (zur Durchführung des Sicherheitstürtests).
Diskrepanzfehler auf Paar 2			Discrepancy Error Pair 2: EIN		
Function Test Error(1)			Function Test Error: EIN		
Synchronization Error			Synchronization Test Error: EIN		

(1) Der Test der Sicherheitstür wurde zwischen zwei Funktionstestsignalen nicht normal durchgeführt.

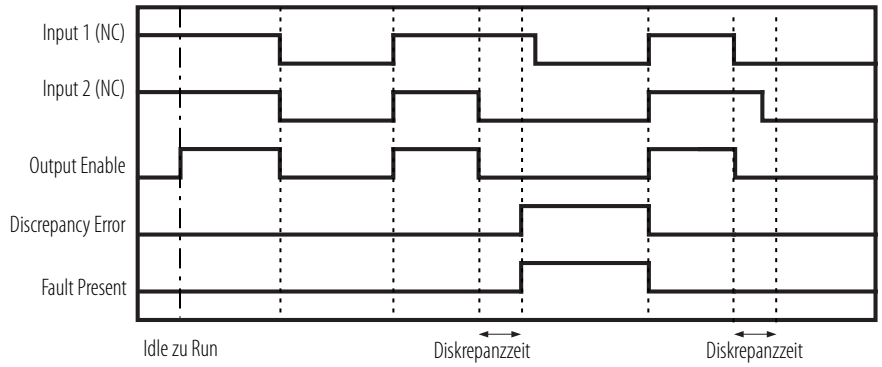
(2) Wenn im Modus Zweikanal-Äquivalent (2 Paare) oder Zweikanal-Komplement (2 Paare) ein Diskrepanzfehler auf einem der Paare auftritt, schalten Sie beide Paare 1 und 2 aus und wieder ein.

Zeitdiagramme für den Funktionsblock „Safety Gate Monitoring“

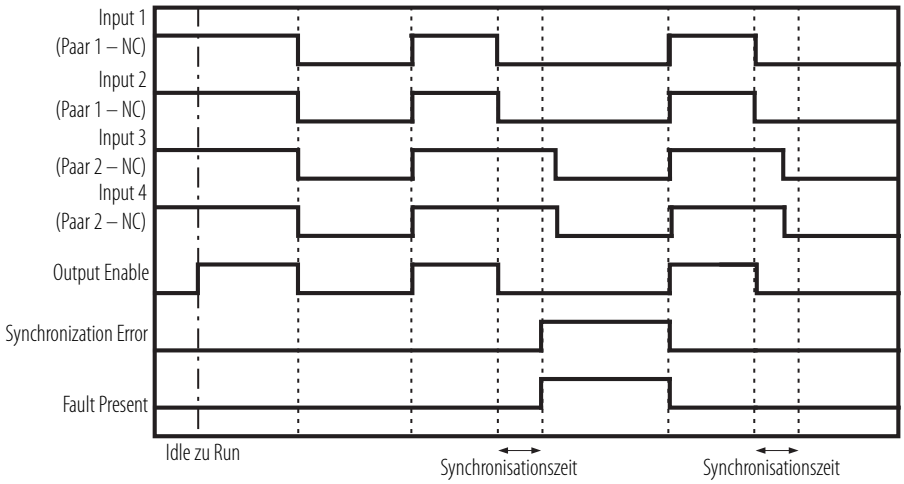
Einkanal bei aktiviertem Funktionstest



Zweikanal-Äquivalent bei deaktiviertem Funktionstest

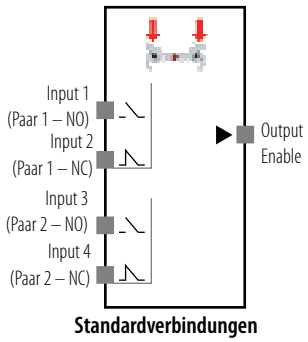


Zweikanal-Äquivalent (2 Paare) bei deaktiviertem Funktionstest

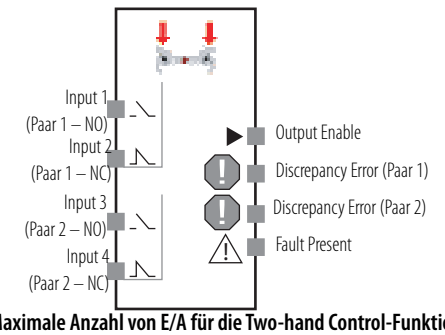


Funktionsblock Two-hand Control (2-Hand-Betätigung)

Diagramme des Funktionsblocks Two-hand Control



Standardverbindungen



Maximale Anzahl von E/A für die Two-hand Control-Funktion

Mit dem Funktionsblock Two-hand Control kann der Zustand eines 2-Hand-Schalters überwacht werden. In Verbindung mit einem geeigneten 2-Hand-Schalter erfüllt der Funktionsblock Two-Hand Control die Anforderungen gemäß Typ III C in EN 574, Zweihandschaltungen – Funktionelle Aspekte; Gestaltungsleitsätze.

Das Ausgangssignal wird nur eingeschaltet, wenn beide Eingänge des 2-Hand-Schalters aktiv sind und die Anforderungen gemäß EN 574 erfüllen. Das Signal „Output Enable“ (Ausgangsaktivierung) wird ausgeschaltet, wenn die Eingänge des 2-Hand-Schalters die Anforderungen gemäß EN 574 nicht erfüllen, einer der Eingänge nicht aktiv ist oder ein Fehler im Funktionsblock registriert wird.

Optionale Ausgänge für den Funktionsblock Two-hand Control

Die optionalen Ausgänge können auch für die Programmierung verwendet werden. Um diese optionalen Ausgänge anzuzeigen, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das entsprechende Kontrollkästchen.

- Discrepancy Error Pair 1
- Discrepancy Error Pair 2

Einstellung des Ausgangs „Fault Present“ für den Funktionsblock Two-hand Control

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Fault Present“ aus.

Parameter des Funktionsblocks Two-hand Control

Stellen Sie diese Parameter für den Funktionsblock „Muting“ ein.

Parameter des Funktionsblocks Two-hand Control

Parameter	Bereich	Standard
Discrepancy Time Input Pair 1 (Diskrepanzzeit Eingang Paar 1)	0 bis 500 ms in Schritten von 10 ms(1) Die Diskrepanzzeiten müssen gleich der oder größer als die Zykluszeit der Steuerung sein.	30 ms
Discrepancy Time Input Pair 2 (Diskrepanzzeit Eingang Paar 2)		

(1) Beim Wert 0 wird keine Prüfung der Diskrepanzzeit durchgeführt.

Wahrheitstabelle für den Funktionsblock Two-hand Control

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für den Funktionsblock Two-hand Control

Input 1 (Paar 1 – NO)	Input 2 (Paar 1 – NC)	Input 3 (Paar 2 – NO)	Input 4 (Paar 2 – NC)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Fehlerbehandlung für den Funktionsblock Two-hand Control

Es wird ein Diskrepanzfehler generiert, wenn sich einer der Eingänge länger als durch die Diskrepanzzeit angegeben in einem nicht korrekten Zustand befindet. Im Modus Zweikanal-Äquivalent müssen beide Eingänge beispielsweise innerhalb der Diskrepanzzeit aktiv (eingeschaltet) sein. Andernfalls wird ein Fehler ausgegeben.

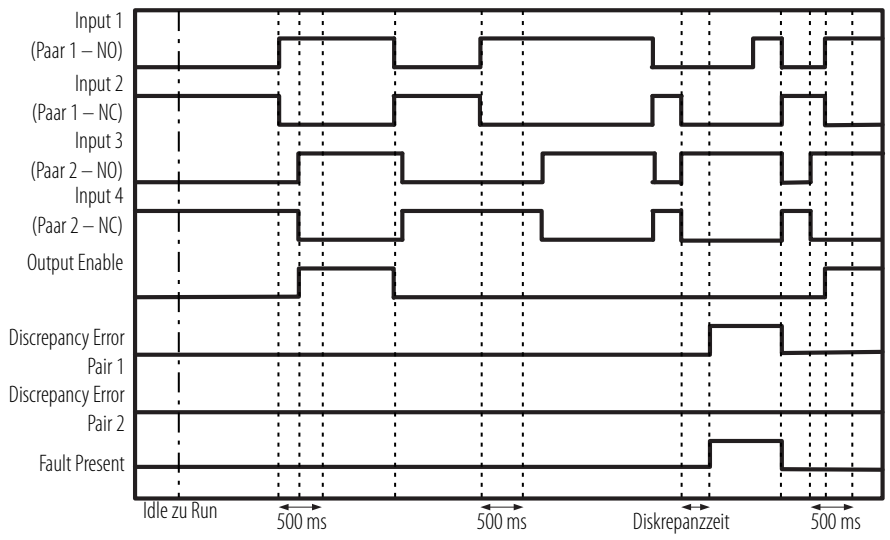
Verwenden Sie diese Tabelle, um Diskrepanzfehler im Funktionsblock Two-hand Control zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks Two-hand Control

Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable[(1)]	Fault Present	Fehler-ausgang	
Diskrepanzfehler auf Paar 1	AUS (Sicherheits-zustand)	EIN	Discrepancy Error Pair 1: EIN	Beseitigen Sie die Ursache für den Fehler und: 1. Schalten Sie beide Eingangspaare 1 und 2 aus und wieder ein. 2. Schalten Sie die Steuerung in den Betriebsmodus „Idle“ (Leerlauf) und wieder zurück nach „Run“ (Betrieb).
Diskrepanzfehler auf Paar 2			Discrepancy Error Pair 2: EIN	

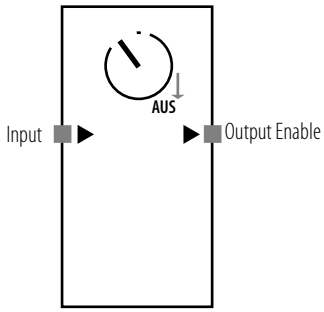
(1) Das Signal „Output Enable“ (Ausgangsaktivierung) wird nicht eingeschaltet, wenn die Synchronisationszeitanforderungen nicht erfüllt sind (d. h., die Betätigung der Eingänge für beide Schalter muss innerhalb von 500 ms erfolgen). Dieser Zustand wird jedoch nicht als Fehler behandelt.

Zeitdiagramm für den Funktionsblock Two-hand Control



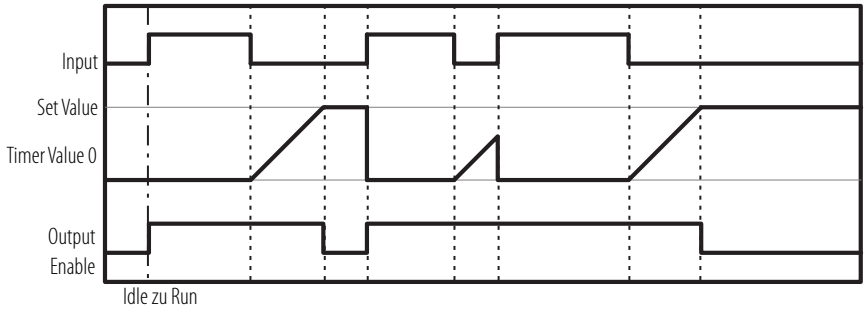
Funktionsblock OFF-delay Timer (Ausschaltverzögerter Timer)

Diagramm des Funktionsblocks OFF-delay Timer



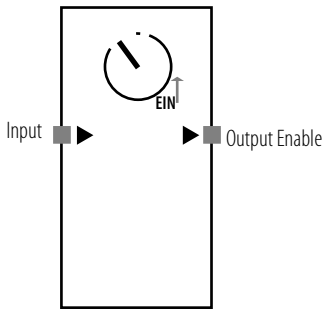
Der Funktionsblock Off-delay Timer stellt einen Timer für eine Ausschaltverzögerung bereit, der in Schritten von 10 ms eingestellt werden kann. Der Bereich für diese Verzögerung liegt bei 0 ms bis 300 Sekunden. Die Standardeinstellung ist 0 ms.

Zeitdiagramm für den Funktionsblock OFF-delay Timer



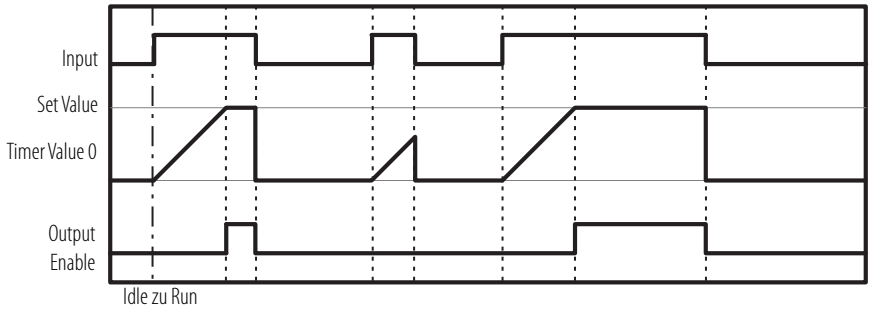
Funktionsblock „ON-delay Timer“ (Einschaltverzögerter Timer)

Diagramm des Funktionsblocks ON-delay Timer



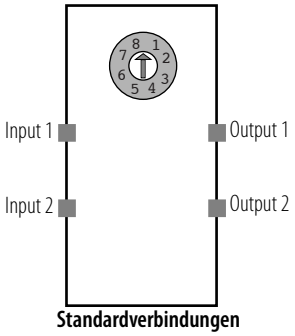
Der Funktionsblock ON-delay Timer stellt einen Timer für eine Einschaltverzögerung bereit, der in Schritten von 10 ms eingestellt werden kann. Der Bereich für diese Verzögerung liegt bei 0 ms bis 300 Sekunden. Die Standardeinstellung ist 0 ms.

Zeitdiagramm für den Funktionsblock ON-delay Timer

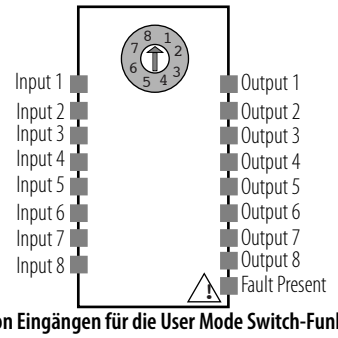


Funktionsblock „User Mode Switch“ (Anwendermodus-Schalter)

Diagramm des Funktionsblocks „User Mode Switch“ (Anwendermodus-Schalter)



Standardverbindungen



Maximale Anzahl von Eingängen für die User Mode Switch-Funktion

Mit dem Funktionsblock User Mode Switch kann ein Betriebsartschalter im Anwendersystem oder -gerät überwacht werden. Ein mit diesem Funktionsblock verbundener Betriebsartschalter muss vom Typ 1-von-N sein, d. h., dass in jedem Fall einer von N Kontakten eingeschaltet ist. Der Funktionsblock unterstützt maximal 8 Eingänge und 8 zugehörige Ausgänge.

Optionale Ausgänge für den Funktionsblock User Mode Switch

Die Anzahl der Ein- und Ausgänge kann im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Settings“ (E/A-Einstellungen) erhöht werden.

Stellen Sie diese Parameter für die optionalen Ausgänge ein.

Optionale Ausgangsparameter für User Mode Switch

Parameter	Bereich	Standard
Number of Inputs (Anzahl der Eingänge)	2 bis 8	2
Number of Outputs (Anzahl der Ausgänge)	2 bis 8	2

Einstellung des Ausgangs „Fault Present“ für den Funktionsblock User Mode Switch

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Settings“ (E/A-Einstellungen) das Kontrollkästchen „Use Fault Present“ (Fault Present verwenden) aus.

Wahrheitstabelle für den Funktionsblock User Mode Switch

In der Wahrheitstabelle steht 0 für AUS und 1 für EIN.

Wahrheitstabelle für den Funktionsblock User Mode Switch

Eingänge								Ausgänge							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

Fehlerbehandlung für den Funktionsblock User Mode Switch

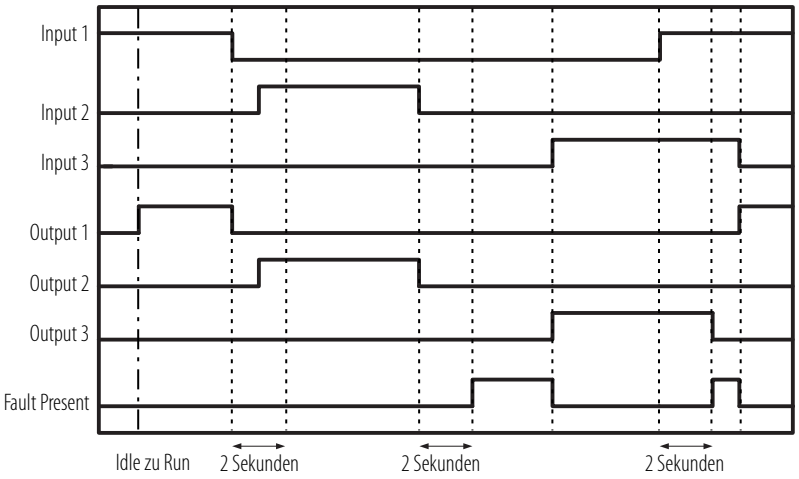
Verwenden Sie diese Tabelle, um Diskrepanzfehler im Funktionsblock User Mode Switch zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks User Mode Switch

Fehlerzustand	Zustand beim Auftreten des Fehlers		Zurücksetzen des Fehlerzustands
	Ausgang	Fault Present	
Mehrere Eingänge waren länger als 2 Sekunden eingeschaltet.(1)	AUS (Sicherheitszustand)	Ein	Überprüfen Sie das System, und stellen Sie sicher, dass jeweils nur ein Kontakt eingeschaltet ist.
Alle Eingänge waren länger als 2 Sekunden ausgeschaltet.			

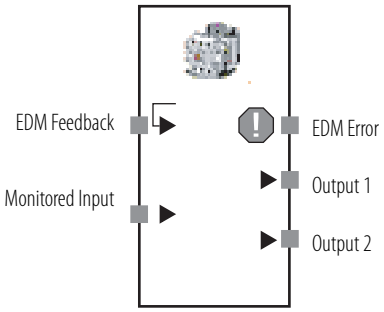
(1) Wenn mehrere Eingänge zur selben Zeit eingeschaltet sind, wird der zugehörige Ausgang für den ersten Eingang für 2 Sekunden eingeschaltet.

Zeitdiagramm für den Funktionsblock User Mode Switch

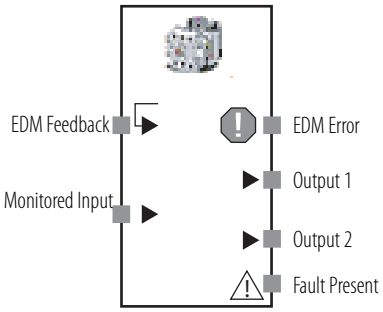


External Device Monitoring (EDM, Externe Geräteüberwachung)

Diagramm des Funktionsblocks External Device Monitoring



Standardverbindungen



Maximale Anzahl von E/A für die EDM-Funktion

Mit dem Funktionsblock External Device Monitoring (EDM) werden das Signal „Monitored Input“ (Überwachter Eingang) und der Zustand des Rückführungssignals eines externen Geräts (EDM Feedback) überwacht. Ausgehend von diesen Signalen werden die Sicherheitsausgänge zu einem externen Gerät eingeschaltet.

Beim Einschalten des Signals „Monitored Input“ werden die Signale „Output 1“ (Ausgang 1) und „Output 2“ (Ausgang 2) eingeschaltet. Nach dem Ausschalten muss innerhalb der angegebenen Zeit der Zustand des Rückführungssignals wechseln. Beim Ausschalten des Signals „Monitored Input“ werden die Signale „Output 1“ und „Output 2“ ausgeschaltet. Nach dem Ausschalten muss innerhalb der angegebenen Zeit der Zustand des Rückführungssignals wechseln.

Wenn der Zustand des Rückführungssignals nicht innerhalb der angegebenen Zeit wechselt, wird ein EDM-Fehler erzeugt: Die Signale „Output 1“ und „Output 2“ werden ausgeschaltet, und das Signal „EDM Error“ wird eingeschaltet.

Optionale Ausgänge für den EDM-Funktionsblock

Die optionalen Ausgänge können auch für die Programmierung verwendet werden. Um diese optionalen Ausgänge zu verwenden, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das entsprechende Kontrollkästchen.

- EDM error
- Output 2

Einstellung des Ausgangs „Fault Present“ für den EDM-Funktionsblock

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Use Fault Present“ aus.

Parameter des EDM-Funktionsblocks

Stellen Sie diese Parameter für den EDM-Funktionsblock ein.

Parameter des EDM-Funktionsblocks

Parameter	Bereich	Standard
EDM Feedback Maximum Time Delay (T_{EDM}) (Maximale Zeitverzögerung für EDM-Rückführung)	100 bis 1000 ms in Schritten von 10 ms	300 ms

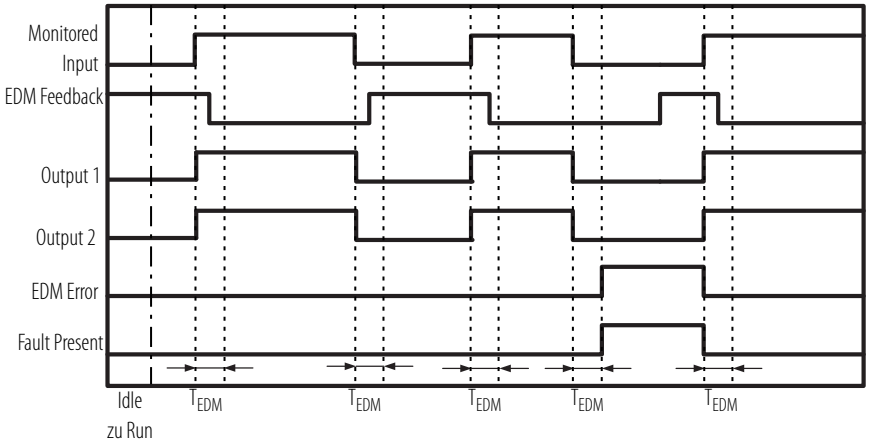
Fehlerbehandlung für den EDM-Funktionsblock

Verwenden Sie diese Tabelle, um Diskrepanzfehler im EDM-Funktionsblock zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des EDM-Funktionsblocks

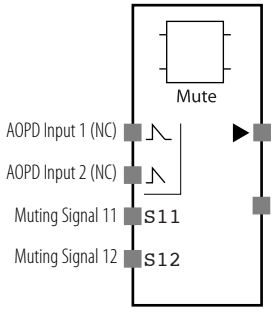
Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehler-ausgang	
EDM Feedback Error (EDM-Rück-führungsfehler)	AUS (Sicherheitszustand)	EIN	EDM Error Output: EIN	Beseitigen Sie die Ursache für den Fehler, und schalten Sie den Sicherheitseingang ein.

Zeitdiagramm für den EDM-Funktionsblock

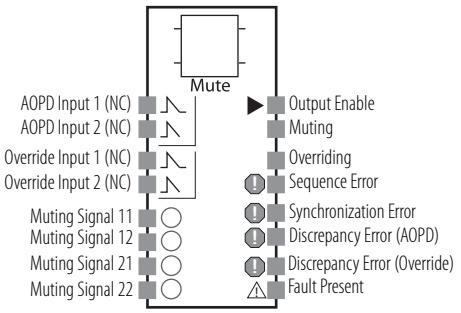


Muting

Diagramme des Funktionsblocks Muting



Standardverbindungen



Maximale Anzahl von E/A für die Muting-Funktion

Mit dem Funktionsblock Muting kann das Lichtunterbrechungssignal (AOPD Input) eines Lichtgitters zeitweilig deaktiviert werden, wenn der Muting-Sensor auslöst. Bei aktivierter Muting-Funktion wird der Maschinenbetrieb nicht unterbrochen, sodass ein Objekt aus der Registrierungszone des Lichtgitters entfernt werden kann. Zusätzlich besitzt der Funktionsblock Muting eine Überbrückungsfunktion, mit der das Lichtunterbrechungssignal des Lichtgitters deaktiviert wird und der Maschinenbetrieb fortgesetzt werden kann, während die Lichter des Lichtgitters verdeckt sind. Wenn beispielsweise ein Objekt die Erfassungszone des Lichtgitters versperrt, kann die Maschine weiterbetrieben werden, um ein Entfernen des Objekts zu ermöglichen.

Parameter des Funktionsblocks Muting

Stellen Sie diese Parameter für den Funktionsblock „Muting“ ein.

Parameter des Funktionsblocks Muting

Parameter	Einstellungen/Bereich	Standard
Muting Mode (Muting-Modus)	• Paralleles Muting mit 2 Sensoren Diese Auswahl eignet sich für Anwendungen am Eingang einer Förderanlage. Verwenden Sie diese Auswahl, wenn zwei retroreflektive, fotoelektrische Sensoren als Muting-Sensoren mit sich überschneidenden Erfassungszonen verwendet werden. • Sequenzielles Muting (Vorwärtsrichtung) Diese Auswahl eignet sich für Anwendungen am Eingang einer Förderanlage. Verwenden Sie diese Auswahl wenn vier Lichtschranken als Muting-Sensoren verwendet werden. • Sequenzielles Muting (beide Richtungen) Diese Auswahl eignet sich für Anwendungen am Eingang oder Ausgang einer Förderanlage. Verwenden Sie diese Auswahl wenn vier Lichtschranken als Muting-Sensoren verwendet werden. • Positionserfassung Diese Auswahl eignet sich für Anwendungen, bei denen das Muting durch einen Schaltereingang gesteuert wird. Verwenden Sie diese Auswahl, um das Lichtunterbrechungssignal des Lichtgitters zeitweilig zu deaktivieren, wenn ein Bediener ein Objekt in eine Öffnung der Maschine einlegt. Hierzu muss sich die Maschine in einem Zustand befinden, in dem keine Gefährdung des Bedieners entsteht. (Die Gefahrenzone der Maschine liegt zu diesem Zeitpunkt in einem anderen Arbeitsbereich.) Bei den Erläuterungen zu allen Einstellungen wird vorausgesetzt, dass die Muting-Sensoren bei einer Erfassung eingeschaltet und bei fehlender Erfassung ausgeschaltet sind.	Paralleles Muting mit 2 Sensoren
Synchronization Time(1) (Synchronisationszeit)	30 ms bis 3 Sekunden in Schritten von 10 ms. Der Einstellwert des Timers muss länger sein als die Zykluszeit der Steuerung.	3 Sekunden
Input Type of AOPD (Eingangstyp für AOPD (Optoelektronische Schutzeinrichtung))	• Zweikanal-Äquivalent (NC/NC) • Zweikanal-Komplement (NC/NO)	Zweikanal-Äquivalent
Discrepancy Time (Diskrepanzzeit) (AOPD)	10 bis 500 ms in Schritten von 10 ms(2) Der Einstellwert des Timers muss länger sein als die Zykluszeit der Steuerung.	30 ms
Input Type of Override Signal (Eingangstyp des Überbrückungssignals)	• Einkanal • Zweikanal-Äquivalent (NO/NO) • Zweikanal-Komplement (NC/NO) • Nicht verwendet	Nicht verwendet
Discrepancy Time (Override) (Diskrepanzzeit (Überbrückung))	10 bis 500 ms in Schritten von 10 ms(2) Der Einstellwert des Timers muss länger sein als die Zykluszeit der Steuerung.	30 ms
Max Muting Time (Max. Muting-Zeit)	500 ms bis 127,5 Sekunden in Schritten von 500 ms. 0 bis 500 ms in Schritten von 10 ms	60 Sekunden
Max Override Time (Max. Überbrückungszeit)	500 ms bis 127,5 Sekunden in Schritten von 500 ms.	60 Sekunden

(1) Zwischen Muting-Signal 11 und Muting-Signal 12 bzw. zwischen Muting-Signal 21 und Muting-Signal 22.

(2) Beim Wert 0 wird keine Prüfung der Diskrepanzzeit durchgeführt.

Optionale Ausgänge für den Funktionsblock Muting

Die optionalen Ausgänge können auch für die Programmierung verwendet werden. Um diese optionalen Ausgänge zu verwenden, aktivieren Sie im Logik-Editor der Software RSNetWorx for DeviceNet im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Setting“ (E/A-Einstellungen) das entsprechende Kontrollkästchen.

- Overriding
- Synchronization error
- Sequence error
- Discrepancy error (AOPD)
- Discrepancy error (Override)

Einstellung des Ausgangs „Fault Present“ für den Funktionsblock Muting

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Setting“ (E/A-Einstellungen) das Kontrollkästchen „Use Fault Present“ (Fault Present verwenden) aus.

Fehlerbehandlung für den Funktionsblock Muting

Verwenden Sie diese Tabelle, um Diskrepanzfehler im Funktionsblock Muting zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks Muting

Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehlerausgang[3]	
Synchronisationsfehler (zwischen Muting-Signal 11 und Muting-Signal 12 bzw. zwischen Muting-Signal 21 und Muting-Signal 22)[1]	EIN[2]	AUS[2]	Synchronization Error: EIN	Wenden Sie das Muting erneut an, oder schalten Sie die Steuerung in den Betriebsmodus „Idle“ (Leerlauf) und wieder zurück nach „Run“ (Betrieb).
Sequence Error (Ablauffehler)			Sequence Error: EIN	
Discrepancy Error (AOPD)	AUS (Sicherheits-zustand)	EIN	Discrepancy Error (AOPD): EIN	Wird zurückgesetzt, wenn beide Eingangssignale des Lichtgitters aus dem Zustand inaktiv nach aktiv wechseln oder wenn Sie die Steuerung in den Betriebsmodus „Idle“ und wieder zurück nach „Run“ schalten.
Discrepancy Error (Override)			Discrepancy Error (Override): EIN	Wird zurückgesetzt, wenn beide Überbrückungssignale (Eingang) aus dem Zustand inaktiv nach aktiv wechseln oder wenn Sie die Steuerung in den Betriebsmodus „Idle“ und wieder zurück nach „Run“ schalten.

(1) Dieser Fehler wird nur registriert, wenn Sequenzielles Muting (beide Richtungen) als Muting-Modus konfiguriert wurde.

(2) Wenn das Lichtgitter aus diesem Fehlerzustand nach inaktiv (kein Licht) wechselt, wird das Signal „Output Enable“ (Ausgangsaktivierung) ausgeschaltet und das Signal „Fault Present“ eingeschaltet. Beim Aktivieren des Lichtgitters (Licht fällt ein) oder Verwenden der Überbrückungsfunktion wird das Signal „Output Enable“ eingeschaltet und das Signal „Fault Present“ ausgeschaltet.

(3) Wenn mehrere Fehler auftreten, werden die Fehler an allen betroffenen Fehlerausgängen angezeigt.

Detailbeschreibung der Muting-Funktion

In den folgenden Abschnitten werden die Start-, Stopp- und Rücksetzbedingungen für den Funktionsblock Muting beschrieben.

Rücksetzbedingungen

Der Sicherheitsausgang (Output Enable) ist eingeschaltet, solange alle folgenden Bedingungen erfüllt sind:

- Das Signal vom Lichtgitter ist aktiv (Licht fällt ein).
- Es ist kein Diskrepanzfehler aufgetreten.

Startbedingungen

Wenn die Muting-Sensoren folgende Bedingungen erfüllen, während das Signal „Output Enable“ (Ausgangsaktivierung) eingeschaltet ist, wird Muting angewendet und das Muting-Signal eingeschaltet:

- Alle Muting-Sensoren sind ausgeschaltet.
- Während die Muting-Sensoren ausgeschaltet sind, erfassen zwei Muting-Sensoren ein Objekt in der vorgeschriebenen Reihenfolge.
- Während die Muting-Sensoren ausgeschaltet sind, liegen die Synchronisationszeiten beider Muting-Sensoren im vorgeschriebenen Bereich. (Die Positionserfassungseinstellung hat hierauf keinen Einfluss.)

Beim Auftreten eines Fehlers wird ein Alarm generiert. Das Ablauffehler-Signal wird eingeschaltet, wenn ein Fehler in der Reihenfolge registriert wird. Das Synchronisationsfehler-Signal wird eingeschaltet, wenn innerhalb der Synchronisationszeit kein Objekt erfasst werden kann. Der Sicherheitsausgang (Output Enable) wird ausgeschaltet, wenn das Signal des Lichtgitters inaktiv ist (kein Licht), bevor die Steuerung in den Muting-Zustand wechselt.

Stoppbedingungen

Wenn bei aktiviertem Muting folgende Bedingungen erfüllt sind, wird das Muting beendet und das Muting-Signal ausgeschaltet:

- Zwei oder mehr Sensoren sind nicht eingeschaltet.
- Die maximale Muting-Zeit ist verstrichen.
- Es ist ein Diskrepanzfehler aufgetreten.

Der Sicherheitsausgang (Output Enable) wird ausgeschaltet, wenn das Lichtgitter bei nicht aktivem Muting verdeckt wird.

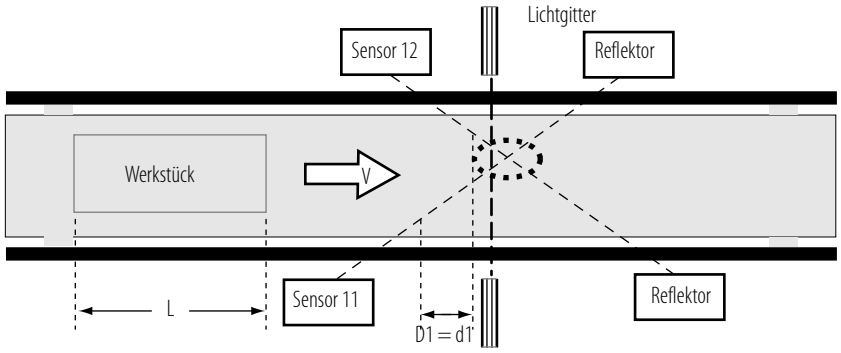
WICHTIG

Wenn die SmartGuard-Steuerung vom Betriebsmodus „Idle" (Leerlauf) in den Modus „Run" (Betrieb) geschaltet wird, bleiben die Eingangsdaten der Slave-Geräte ausgeschaltet, bis die Kommunikation vollständig hergestellt wurde. Wenn Slave-Eingangsdaten für den Eingang „AOPD Input" verwendet werden, werden die Ausgänge „Fault Present" und „Sequence Error" (Ablauffehler) unmittelbar nach dem Wechsel in den Betriebsmodus „Run" eingeschaltet. Mit dem Einschalten des Eingangs „AOPD Input" wird der Ausgang „Fault Present" ausgeschaltet. Sobald die Muting-Startbedingung erfüllt ist, wird der Ausgang „Sequence Error" ausgeschaltet.

Beispiel: Paralleles Muting mit 2 Sensoren

In diesem Beispiel wurden zwei retroreflektive, fotoelektrische Sensoren als Muting-Sensoren mit sich überschneidenden Erfassungszonen installiert. Der Schnittpunkt der beiden Sensoren muss hinter dem Lichtgitter liegen. Verwenden Sie diese Konfiguration, wenn die Längen der Werkstücke (L) variabel oder nicht lang genug sind, um sequenzielle Muting-Sensoren zu aktivieren.

Anwendungskonfiguration



Sensor 12 ist mit Muting-Signal 12 und Sensor 11 mit Muting-Signal 11 verbunden.

Muting-Reihenfolge

In diesem Beispiel wird die Muting-Reihenfolge beschrieben.

1. Das Licht zwischen den Sensoren 11 und 12 sowie dem Lichtgitter wird nicht unterbrochen, das Signal „Output Enable" (Ausgangsaktivierung) ist eingeschaltet.

2. Wenn sich das Werkstück nach rechts bewegt und die Sensoren 11 und 12 in der vorgeschriebenen Reihenfolge eingeschaltet werden, wird das Muting aktiviert.

3. Während sich das Werkstück weiterbewegt, bleibt das Signal „Output Enable“ auch bei verdecktem Lichtgitter eingeschaltet.

4. Das Werkstück verlässt daraufhin den Erfassungsbereich von Sensor 11, womit der Muting-Zustand beendet ist und das Muting-Signal ausgeschaltet wird.

Entfernungseinstellungen

Beim Einrichten dieser Art der Muting-Anwendung muss durch entsprechend gewählte Entfernungseinstellungen ein Auslösen der Muting-Funktion durch eine vorbeigehende Person verhindert werden. Lichtgitter und Muting-Sensoren müssen so eingestellt werden, dass ein Werkstück alle Muting-Sensoren passiert, bevor das nächste Werkstück die Sensoren erreicht.

Die geeigneten Entfernungen für dieses Beispiel können Sie mit folgenden Formeln berechnen, wobei gilt:

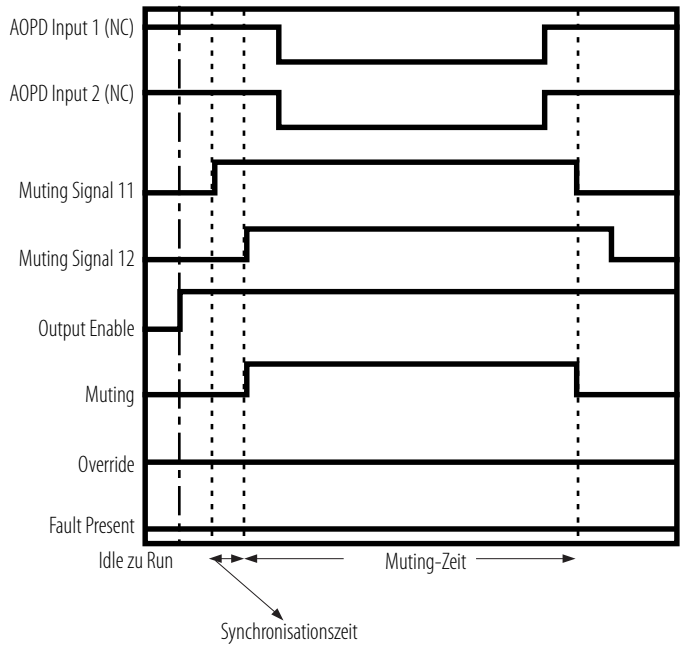
D1 = minimaler erforderlicher Abstand für eine korrekte Muting-Sensorleistung
d1 = maximal zulässiger Abstand für eine korrekte Muting-Sensorleistung
L = Länge des Werkstücks
V = Geschwindigkeit des Werkstücks
T1min = Zykluszeit der Steuerung
T1max= Einstellung der Synchronisationszeit (Standardwert ist 3 Sekunden)

Formel 1: $D1 < L$
Formel 2: $V \times T1min < d1 < V \times T1max$

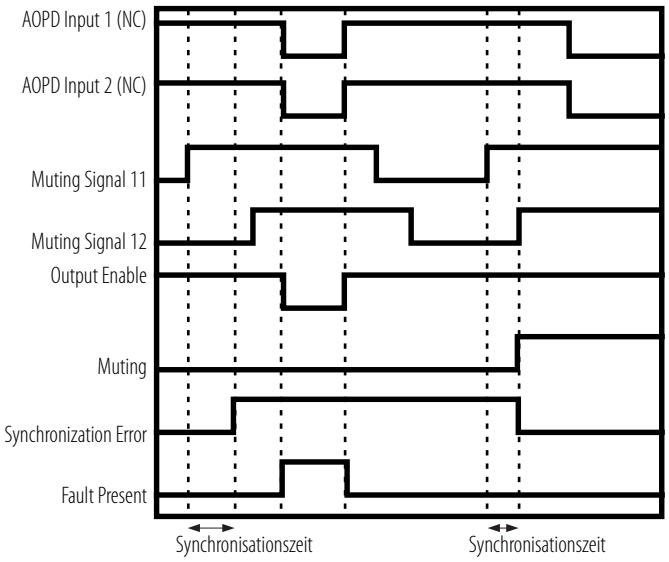
Für einen effektiven und ordnungsgemäßen Betrieb der Muting-Funktion müssen beide Formeln erfüllt werden.

Zeitdiagramm für sequenzielles Muting (Vorwärtsrichtung)

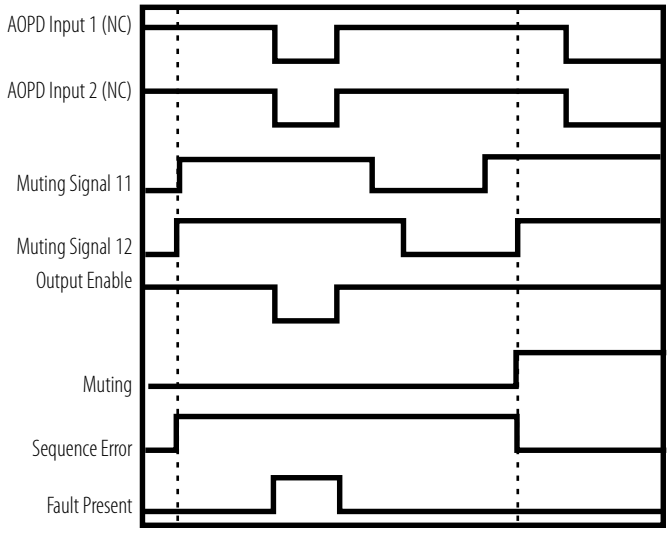
Normaler Betrieb



Synchronisationsfehler



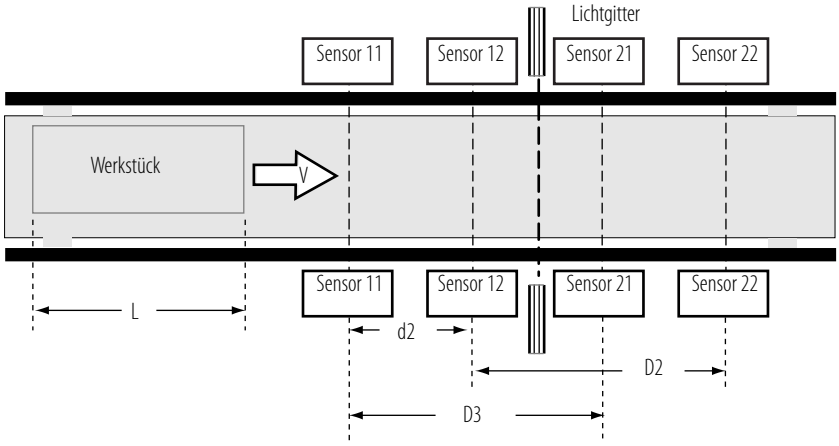
Ablauffehler



Beispiel: Sequenzielles Muting mit 4 Sensoren (Vorwärtsrichtung)

In diesem Beispiel wurden vier fotoelektrische Sensoren mit durchgehenden Strahlen als Muting-Sensoren installiert. Verwenden Sie diese Konfiguration, wenn die Längen der transportierten Werkstücke (L) gleichbleibend und groß genug sind, um sequenziell installierte Muting-Sensoren zu aktivieren.

Anwendungskonfiguration



Sensor 11 ist verbunden mit Muting-Signal 11, Sensor 12 mit Muting-Signal 12, Sensor 21 mit Muting-Signal 21 und Sensor 22 mit Muting-Signal 22.

Muting-Reihenfolge

Im Folgenden wird die Muting-Reihenfolge für dieses Beispiel beschrieben.

1. Das Licht zwischen den Sensoren 11, 12, 21 und 22 und dem Lichtgitter wird nicht unterbrochen, das Signal „Output Enable“ (Ausgangsaktivierung) ist eingeschaltet.

2. Wenn sich das Werkstück nach rechts bewegt und die Sensoren 11 und 12 in der vorgeschriebenen Reihenfolge eingeschaltet werden, wird das Muting aktiviert und das Muting-Signal eingeschaltet.

3. Während sich das Werkstück weiterbewegt, bleibt das Signal „Output Enable“ auch bei verdecktem Lichtgitter eingeschaltet.

4. Das Werkstück verlässt schließlich den Erfassungsbereich von Sensor 21, womit der Muting-Zustand beendet ist und das Muting-Signal ausgeschaltet wird.

Entfernungseinstellungen

Beim Einrichten dieser Art der Muting-Anwendung muss durch entsprechend gewählte Entfernungseinstellungen ein Auslösen der Muting-Funktion durch eine vorbeigehende Person verhindert werden. Lichtgitter und Muting-Sensoren müssen so eingestellt werden, dass ein Werkstück alle Muting-Sensoren passiert, bevor das nächste Werkstück die Sensoren erreicht.

Die geeigneten Entfernungen für dieses Beispiel können Sie mit folgenden Formeln berechnen, wobei gilt:

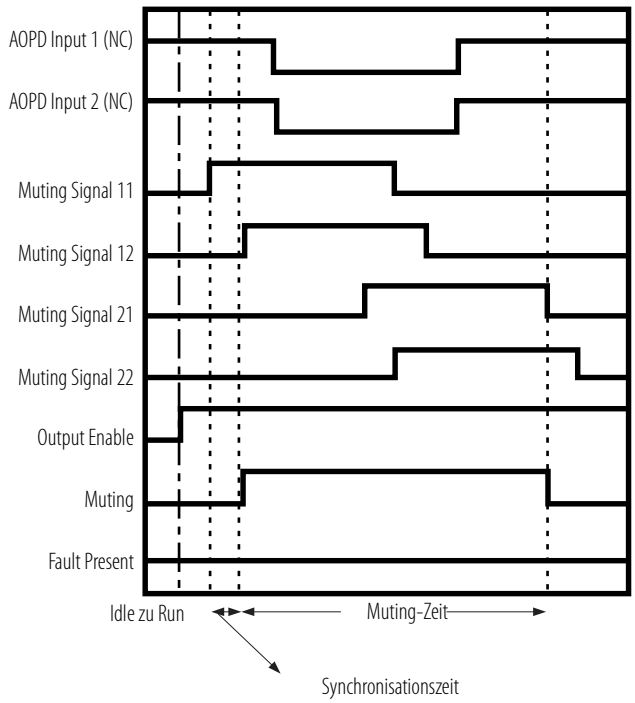
D2 und D3 = minimaler erforderlicher Abstand für eine korrekte Muting-Sensorleistung
d2 = maximal zulässiger Abstand für eine korrekte Muting-Sensorleistung
L = Länge des Werkstücks
V = Geschwindigkeit des Werkstücks
T1min = Zykluszeit der Steuerung
T1max= Einstellung der Synchronisationszeit (Standardwert ist 3 Sekunden)

Formel 3: $D2 < L$
Formel 4: $D3 < L$
Formel 5: $V \times T1min < d2 < V \times T1max$

Für einen effektiven und ordnungsgemäßen Betrieb der Muting-Funktion müssen Formeln 3, 4 und 5 erfüllt werden.

Zeitdiagramm für sequenzielles Muting (Vorwärtsrichtung)

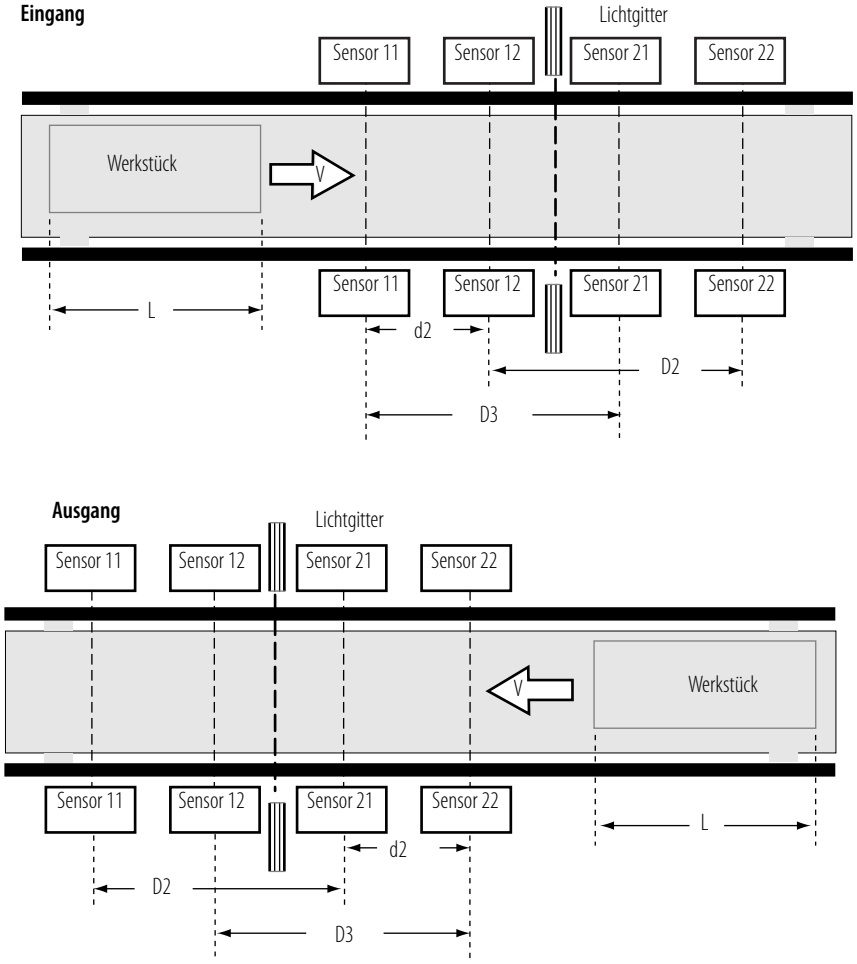
Normaler Betrieb



Beispiel: Sequenzielles Muting mit 4 Sensoren (beide Richtungen)

In diesem Beispiel wurden vier fotoelektrische Sensoren mit durchgehenden Strahlen als Muting-Sensoren installiert.

Anwendungskonfiguration



Sensor 11 ist verbunden mit Muting-Signal 11, Sensor 12 mit Muting-Signal 12, Sensor 21 mit Muting-Signal 21 und Sensor 22 mit Muting-Signal 22.

Muting-Reihenfolge

Im Folgenden wird die Muting-Reihenfolge für dieses Beispiel beschrieben.

1. Das Licht zwischen den Sensoren 11, 12, 21 und 22 und dem Lichtgitter wird nicht unterbrochen, das Signal „Output Enable“ (Ausgangsaktivierung) ist eingeschaltet.

2. Eingang: Wenn sich das Werkstück nach rechts bewegt und die Sensoren 11 und 12 in der vorgeschriebenen Reihenfolge eingeschaltet werden (Sensoren 21 und 22 werden beim Verlassen des Werkstücks eingeschaltet), wird das Muting aktiviert und das Muting-Signal eingeschaltet.

3. Während sich das Werkstück weiterbewegt, bleibt das Signal „Output Enable“ auch bei verdecktem Lichtgitter eingeschaltet.

4. Das Werkstück verlässt schließlich den Erfassungsbereich von Sensor 21 am Anfang (Sensor 12 beim Verlassen des Werkstücks), womit der Muting-Zustand beendet ist und das Muting-Signal ausgeschaltet wird.

Entfernungseinstellungen

Beim Einrichten dieser Art der Muting-Anwendung muss durch entsprechend gewählte Entfernungseinstellungen ein Auslösen der Muting-Funktion durch eine vorbeigehende Person verhindert werden. Lichtgitter und Muting-Sensoren müssen so eingestellt werden, dass ein Werkstück alle Muting-Sensoren passiert, bevor das nächste Werkstück die Sensoren erreicht.

Die geeigneten Entfernungen für dieses Beispiel können Sie mit folgenden Formeln berechnen, wobei gilt:

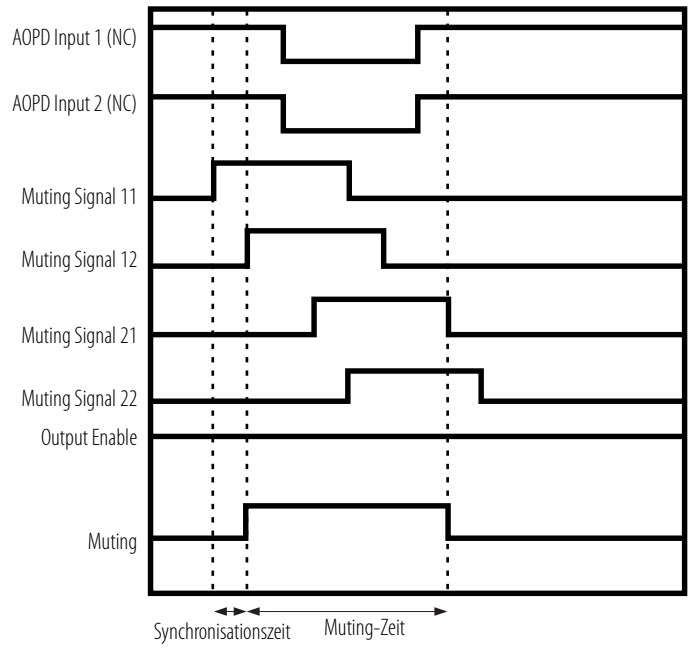
D2 und D3 = minimaler erforderlicher Abstand für eine korrekte Muting-Sensorleistung
d2 = maximal zulässiger Abstand für eine korrekte Muting-Sensorleistung
L = Länge des Werkstücks
V = Geschwindigkeit des Werkstücks
T1min = Zykluszeit der Steuerung
T1max= Einstellung der Synchronisationszeit
(Standardwert ist 3 Sekunden)

Formel 3: D2 < L
Formel 4: D3 < L
Formel 5: V x T1min < d2 < V x T1max

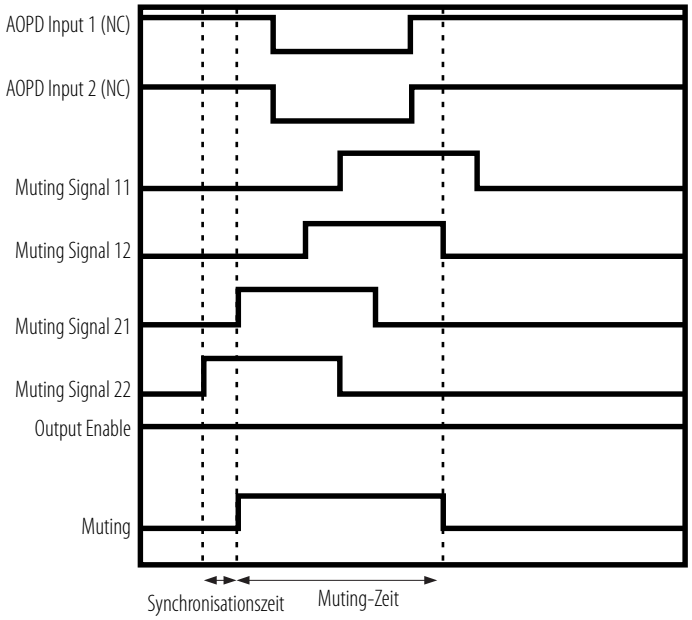
Für einen effektiven und ordnungsgemäßen Betrieb der Muting-Funktion müssen Formeln 3, 4 und 5 erfüllt werden.

Zeitdiagramme für sequenzielles Muting (beide Richtungen)“

Eingangszeitdiagramm



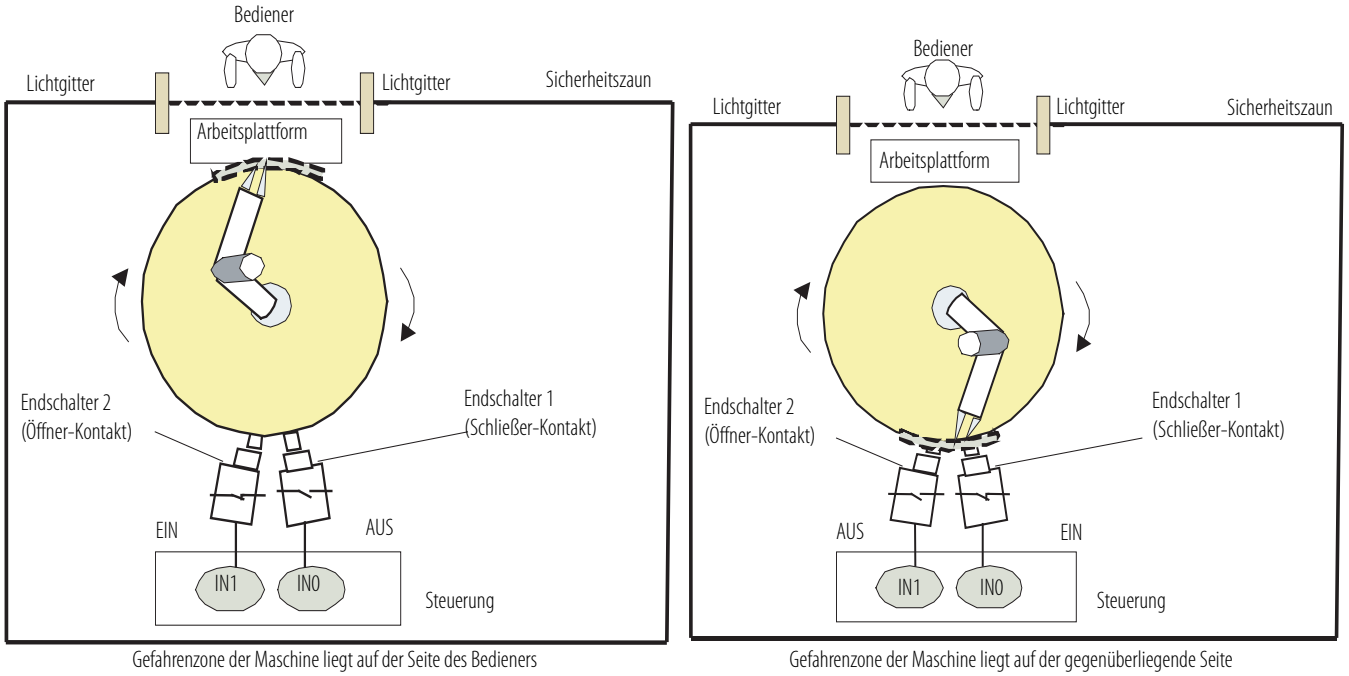
Zeitdifferenz Eingangsmuster 2: Ausgangszeitdiagramm



Beispiel: Positionserfassung

Bei dieser Beispielanwendung wird das Werkstück auf die Drehscheibe einer Maschine gesetzt, die von einem Sicherheitszaun umgeben ist. Der Bediener kann das Lichtunterbrechungssignal des Sicherheitslichtgitters deaktivieren, um ein Werkstück auf die Drehscheibe zu setzen, wenn sich die Gefahrenzone der Maschine auf der gegenüberliegenden Seite des Bedieners befindet.

Anwendungskonfiguration

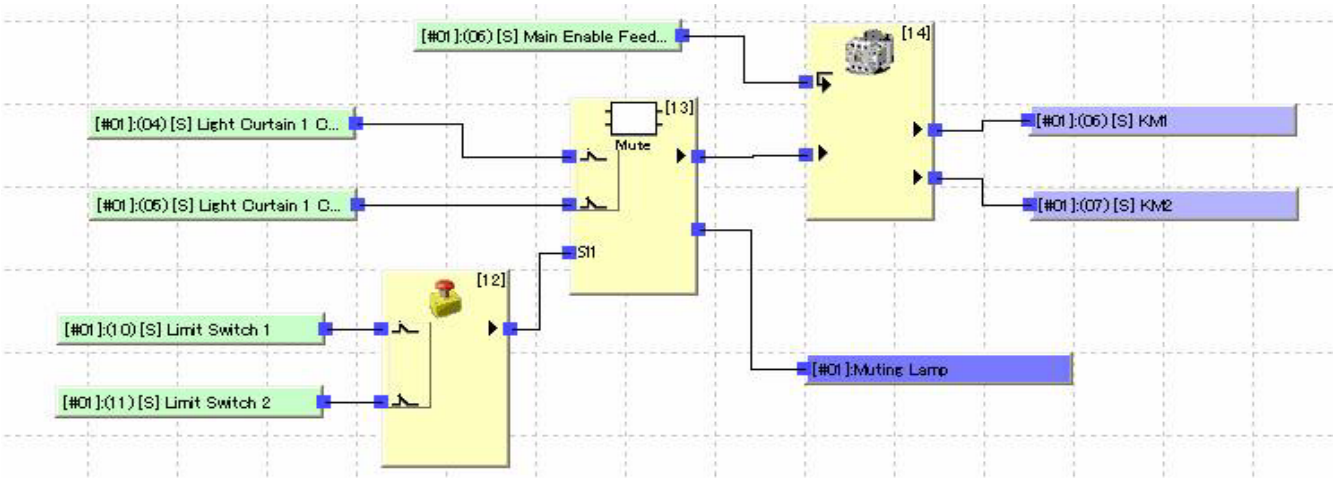


Konfigurieren Sie den zentralen Eingang in der Steuerung als Zweikanal-Komplementär.

Programmierungsbeispiel

Endschalter 1 und 2 sind über einen ESTOP-Befehl mit Muting-Signal 11 des Muting-Funktionsblocks verbunden. Für die Endschalter 1 und 2 wurde die Einstellung Zweikanal-Komplementär für die zentralen Eingänge gewählt, um die Eingangsdaten beider Schalter auszuwerten.

Programmierlogik



Muting-Reihenfolge

Im Folgenden wird die Muting-Reihenfolge für dieses Beispiel beschrieben.

1. Wenn die Gefahrenzone der Maschine auf Seite des Bedieners liegt, ist Schließer-Endschalter 1 ausgeschaltet und Öffner-Endschalter 2 eingeschaltet. Außerdem wird das Lichtgitter nicht verdeckt, das Signal „Output Enable“ (Ausgangsaktivierung) ist eingeschaltet. Muting-Signal 11, das Zweikanal-Komplementär-Signal für Endschalter 1 und 2, wird ausgeschaltet.

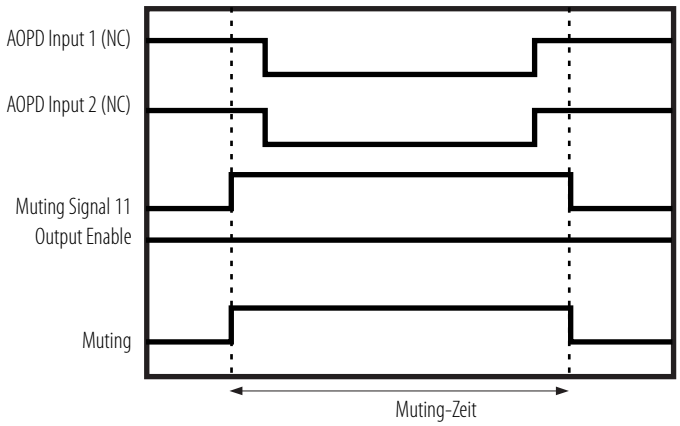
2. Wenn sich der Roboterarm dreht, wird Endschalter 1 eingeschaltet und Endschalter 2 ausgeschaltet, sobald die Gefahrenzone gegenüber dem Bediener liegt. Das Ergebnis des ESTOP-Befehls, welches das Zweikanal-Komplementär-Signal für Endschalter 1 und 2 liefert, wird eingeschaltet, sodass das Muting aktiviert und das Muting-Signal eingeschaltet wird.

3. Zu diesem Zeitpunkt bleibt das Signal „Output Enable“ auch bei verdecktem Lichtgitter eingeschaltet, sodass der Bediener die Arbeitsplattform erreichen kann.

4. Wenn der Bediener seine Aufgabe beendet hat und das Lichtgitter bei der anschließenden Bewegung des Roboterarms nicht mehr verdeckt ist, wird das Ergebnis des ESTOP-Befehls ausgeschaltet, der Muting-Zustand wird beendet und das Muting-Signal ausgeschaltet.

Zeitdiagramm

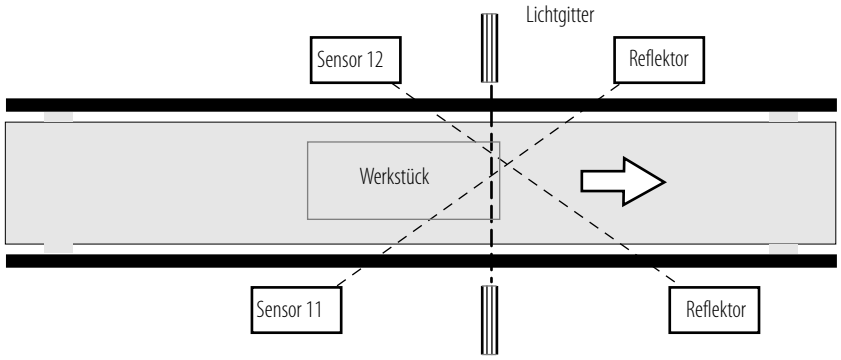
Normaler Betrieb



Beispiel: Überbrückungsfunktion

Mit der Überbrückungsfunktion kann der Sicherheitsausgang auch dann eingeschaltet werden, wenn das Lichtunterbrechungssignal des Lichtgitters nicht aktiv ist. Wenn ein Werkstück beim Transport stecken bleibt, kann der ordnungsgemäße Betrieb des Systems nur wiederhergestellt werden, indem das Werkstück entfernt wird. In einer solchen Situation kann die Überbrückungsfunktion verwendet werden, um das Werkstück aus der Erfassungszone des Lichtgitters zu entfernen.

Anwendungskonfiguration



Sensor 11 ist mit Muting-Signal 11 und Sensor 12 mit Muting-Signal 12 verbunden.

Überbrückungsreihenfolge

Im Folgenden wird die Überbrückungsreihenfolge für dieses Beispiel beschrieben.

1. Das Signal „Output Enable“ (Ausgangsaktivierung) ist ausgeschaltet.

2. Durch Einschalten der Überbrückungseingänge wird die Überbrückungsfunktion aktiviert und das Überbrückungssignal eingeschaltet. Während die Überbrückungseingänge eingeschaltet sind, wird der Muting-Zustand erzwungen, und das Muting-Signal und das Signal „Output Enable“ bleiben eingeschaltet.

3. Wenn sich das Werkstück nach rechts bewegt und nicht mehr vom Sensor (hier: Sensor 12) erfasst wird, wird der durch die Überbrückungsfunktion erzwungene Muting-Zustand beendet, und das Muting-Signal sowie das Signal „Output Enable“ werden ausgeschaltet.

Startbedingungen für die Überbrückungsfunktion

Wenn die folgenden Bedingungen erfüllt sind, wird die Überbrückungsfunktion gestartet, und die Signale „Output Enable“, „Muting“ und „Override“ werden eingeschaltet.

- Mindestens ein Muting-Sensor ist eingeschaltet.
- Das Lichtgitter ist nicht aktiv (verdeckt).
- Das Signal „Output Enable“ ist ausgeschaltet.
- Das Signal „Override Input“ (Überbrückungseingang) ist eingeschaltet (bei einer Konfiguration mit einem einzelnen Eingang) bzw. aktiv (bei einer Konfiguration mit zwei Eingängen).

Stoppbedingungen für die Überbrückungsfunktion

Wenn eine der folgenden Bedingungen erfüllt ist, wird die Überbrückungsfunktion gestoppt, und die Signale „Muting“ und „Override“ werden ausgeschaltet.

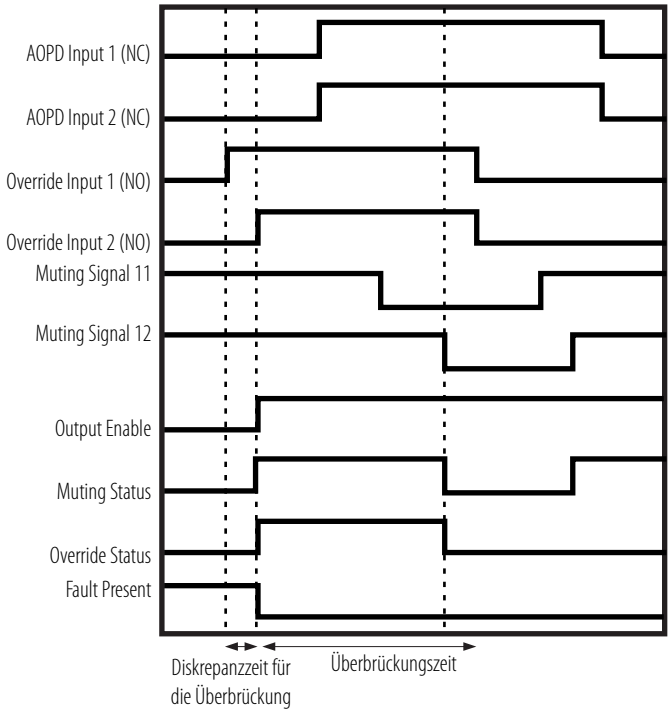
- Alle Muting-Signale sind ausgeschaltet.
- Die maximale Überbrückungszeit ist verstrichen.
- Das Signal „Override Input“ ist ausgeschaltet (bei einer Konfiguration mit einem einzelnen Eingang) bzw. inaktiv (bei einer Konfiguration mit zwei Eingängen).

Beim Beenden der Überbrückungsfunktion wird „Output Enable“ ausgeschaltet, falls das Lichtgitter verdeckt ist.

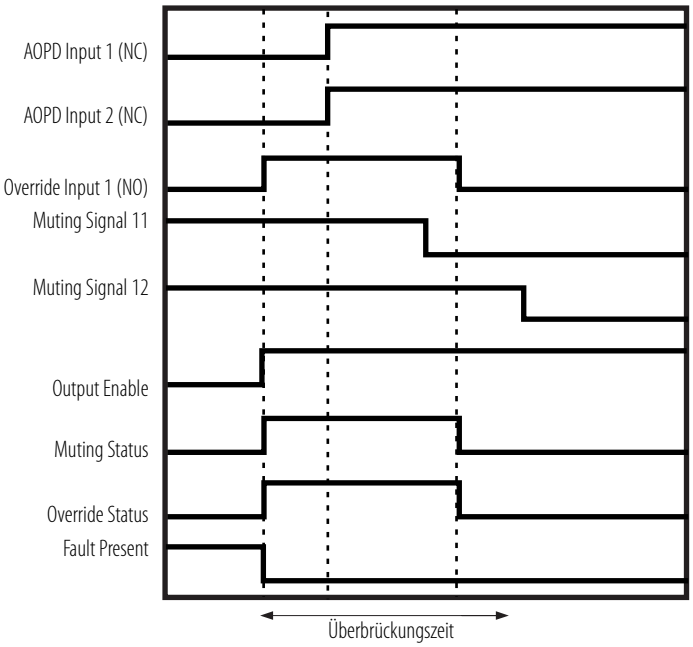
Zeitdiagramm

Bei den folgenden Diagrammen wird als Muting-Modus das parallele Muting mit 2 Sensoren verwendet.

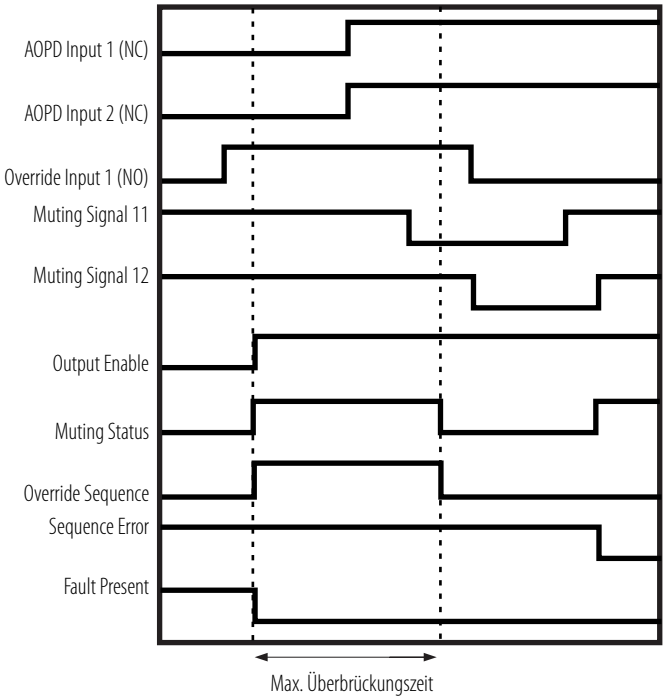
Normaler Betrieb der Überbrückungsfunktion



Überbrückungssignal wird während der Überbrückung ausgeschaltet

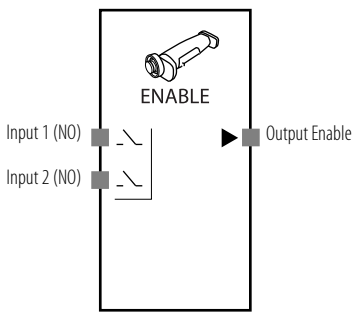


Überbrückungs-Timeout während der Überbrückung

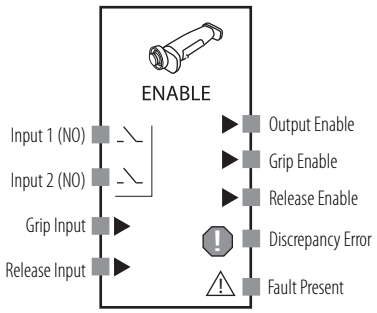


Enable Switch (Zustimmschalter)

Diagramm des Funktionsblocks Enable Switch



Standardverbindungen



Maximale Anzahl von E/A für die Enable Switch-Funktion

Mit dem Funktionsblock Enable Switch wird der Zustand des Zustimmschaltergeräts überwacht. Das Signal „Output Enable“ (Ausgangsaktivierung) ist eingeschaltet, wenn die Eingänge des überwachten Zustimmschalters aktiv sind. Das Signal „Output Enable“ wird ausgeschaltet, wenn die Eingänge nicht aktiv sind oder für den Funktionsblock ein Fehler registriert wird.

Wenn der Zustimmschalter zusätzlich ein Verriegelungssignal und ein Entriegelungssignal unterstützt, kann der Zustand der beiden Signale „Grip Input“ (Verriegelungseingang) und „Release Input“ (Entriegelungseingang) ebenfalls überwacht werden. Die empfangenen Signale „Grip Input“ und „Release Input“ beeinflussen jedoch nicht den Zustand des Signals „Output Enable“.

Parameter des Funktionsblocks Enable Switch

Stellen Sie diese Parameter für den Funktionsblock „Enable Switch“ ein.

Parameter des Funktionsblocks Enable Switch

Parameter	Gültiger Bereich	Standardeinstellung
Input Type (Eingangstyp)	Einkanal Zweikanal-Äquivalent	Zweikanal-Äquivalent
Discrepancy Time (Diskrepanzzeit)	0 bis 30 s in Schritten von 10 ms.(1) Die Diskrepanzzeit muss gleich oder größer als die Zykluszeit der Steuerung sein.	30 ms

(1) Wenn die Diskrepanzzeit auf 0 eingestellt wird, erfolgt keine Überprüfung.

In der Software RSNetWorx for DeviceNet kann die Anzahl der Eingänge im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „In/Out Settings“ (E/A-Einstellungen) von zwei auf vier erhöht werden. Auch wenn als Eingangstyp Einkanal ausgewählt wird, sind zwei Eingänge vorhanden. Die Signale „Grip Input“ (Verrieglungseingang) und „Release Input“ (Entriegelungseingang) können bei Auswahl von drei oder vier Eingängen verwendet werden. Die Standardeinstellung ist zwei.

Optionale Ausgänge

Die optionalen Ausgänge können auch für die Programmierung verwendet werden. Um diese optionalen Ausgänge zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) die Kontrollkästchen für die entsprechenden Ausgänge aus.

- Grip enable
- Release enable
- Discrepancy error

Einstellung des Ausgangs „Fault Present“

Der Ausgang „Fault Present“ kann auch für die Programmierung verwendet werden. Um diesen Ausgang zu aktivieren, wählen Sie im Dialogfeld „Function Block Properties“ (Eigenschaften des Funktionsblocks) auf der Registerkarte „Out point“ (Ausgangspunkt) das Kontrollkästchen „Fault Present“ aus.

Fehlerbehandlung für den Funktionsblock Enable Switch

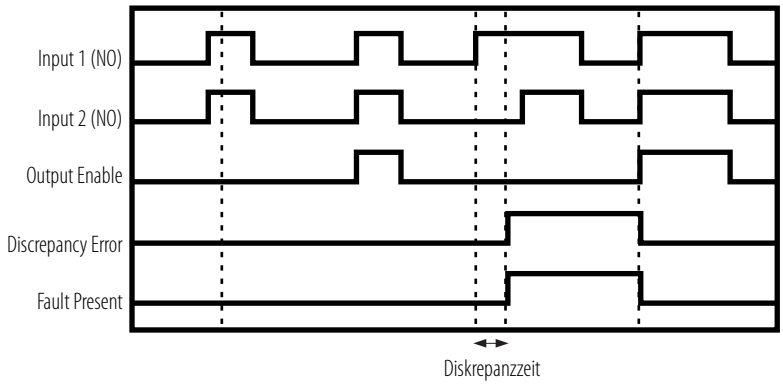
Verwenden Sie diese Tabelle, um einen Diskrepanzfehler im Funktionsblock Enable Switch zu untersuchen und zurückzusetzen.

Fehlererkennung und Zurücksetzen des Funktionsblocks Enable Switch

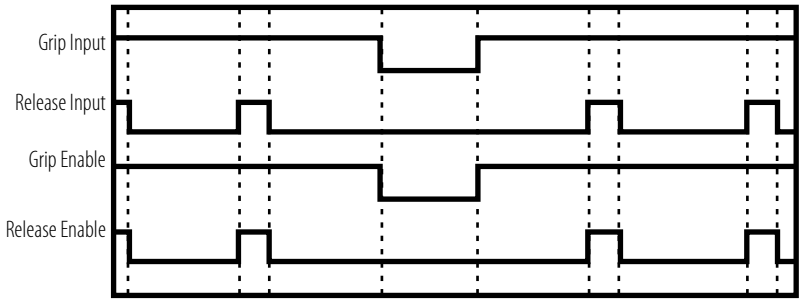
Fehlerzustand	Zustand beim Auftreten des Fehlers			Zurücksetzen des Fehlerzustands
	Output Enable	Fault Present	Fehler-ausgang	
Diskrepanzfehler auf Eingangspaar	AUS (Sicherheitszustand)	EIN	Discrepancy Error: EIN	Beseitigen Sie die Ursache für den Fehler und: 1. Schalten Sie beide Eingangspaare 1 und 2 aus und wieder ein. 2. Schalten Sie die Steuerung in den Betriebsmodus „Idle“ (Leerlauf) und wieder zurück nach „Run“ (Betrieb).

Zeitdiagramme für den Funktionsblock Enable Switch

Normaler Betrieb und Diskrepanzfehler

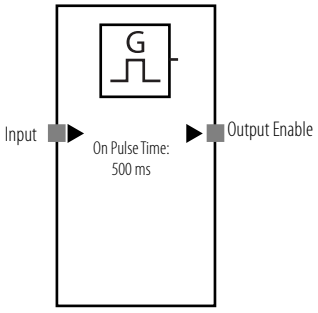


Verriegelungssignal und Entriegelungssignal



Pulse Generator (Impulsgenerator)

Diagramm des Funktionsblocks Pulse Generator



Der Funktionsblock Pulse Generator (Impulsgenerator) erzeugt einen Ein/Aus-Impuls am Signal „Output Enable“ (Ausgangsaktivierung), solange das Eingangssignal des Funktionsblocks eingeschaltet ist.

Die Intervalle der Zustände EIN und AUS können unabhängig voneinander zwischen 10 ms und 3 Sekunden in Schritten von 10 ms eingestellt werden. Wenn die Intervallzeit für den Zustand EIN auf 100 ms und die Zeit für den Zustand AUS auf 500 ms eingestellt ist, wird das Signal kontinuierlich jeweils für 100 ms eingeschaltet und anschließend für 500 ms ausgeschaltet.

Die Ausgangsimpulsweite unterliegt einer zeitlichen Abweichung, die der Zykluszeit der SmartGuard-Steuerung entspricht. Wenn die Zykluszeit der SmartGuard-Steuerung beispielsweise 7 ms beträgt und die Impulsweite auf 100 ms eingestellt wurde, liegt die tatsächliche Ausgangsimpulsweite zwischen 93 und 107 ms.

Parameter des Funktionsblocks Pulse Generator

Stellen Sie diese Parameter für den Funktionsblock Pulse Generator ein.

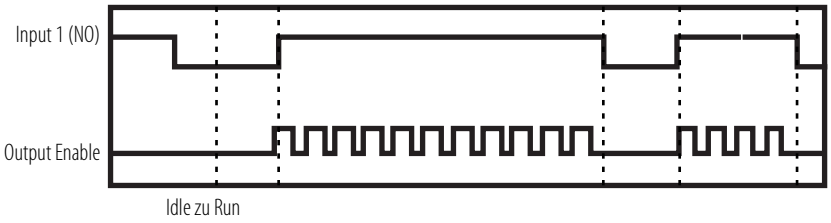
Parameter des Funktionsblocks Pulse Generator

Parameter	Gültiger Bereich	Standardeinstellung
On pulse time (Impulszeit EIN)	10 ms bis 3 s in Schritten von 10 ms(1)	500 ms
Off pulse time (Impulszeit AUS)	10 ms bis 3 s in Schritten von 10 ms(1)	500 ms

(1) Der Einstellwert muss länger sein als die Zykluszeit der Steuerung.

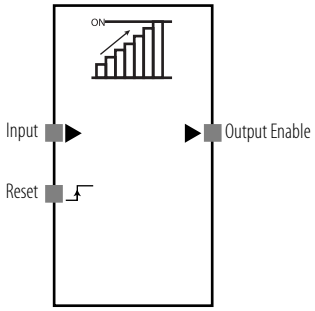
Zeitdiagramm für den Funktionsblock Pulse Generator

Zeitdiagramm für Pulse Generator



Counter (Zähler)

Diagramm des Funktionsblocks Counter



Der Funktionsblock „Counter“ (Zähler) zählt die Eingangsimpulse an einem Eingang und schaltet das Signal „Output Enable“ (Ausgangsaktivierung) ein, sobald der Zähler einen Sollwert erreicht. Dieser Wert wird in der Software RSNetWorx for DeviceNet eingestellt.

Sobald die Zählung der Eingangsimpulse den Sollwert erreicht, wird das Signal „Output Enable“ eingeschaltet und bleibt eingeschaltet. Zur Registrierung von Eingangsimpulsen müssen die Impulszeiten beider Signalzustände (EIN und AUS) am Eingang länger sein als die Zykluszeit der Steuerung. Wenn die Impulszeit eines oder beider Eingangssignalzustände kürzer ist als die Zykluszeit der Steuerung, werden einige Impulse unter Umständen nicht gezählt.

Parameter des Funktionsblocks Counter

Stellen Sie diese Parameter für den Funktionsblock Counter ein.

Parameter des Funktionsblocks Counter

Parameter	Gültiger Bereich	Standardeinstellung
Reset condition (Rücksetzbedingung)	Automatische Rücksetzung Manuelle Rücksetzung	Manuelle Rücksetzung
Count type (Zähltyp)	Abwärtszählung (abnehmend) Aufwärtszählung (zunehmend)	Abwärtszählung (abnehmend)
Counter (Zähler)	1 bis 65 535 Zählwerte	1 Zählwert

Rücksetzbedingung

Die Bedingung für das Zurücksetzen des Zählers kann auf manuelle oder automatische Rücksetzung eingestellt werden. Wenn die automatische Rücksetzung ausgewählt wurde und die Eingangsimpulszählung den Sollwert erreicht, wird das Signal „Output Enable“ (Ausgangsaktivierung) eingeschaltet und bleibt eingeschaltet, solange ein Eingangssignal vorhanden ist. Beim Ausschalten des Eingangssignals wird der Zähler zurückgesetzt.

Wenn die manuelle Rücksetzung ausgewählt wurde, wird die Eingangsimpulszählung zurückgesetzt das Signal „Output Enable“ ausgeschaltet, sobald das Signal „Reset“ (Rücksetzung) eingeschaltet wird. Während das Signal „Reset“ eingeschaltet ist, werden keine Eingangsimpulse gezählt.

Zähltyp

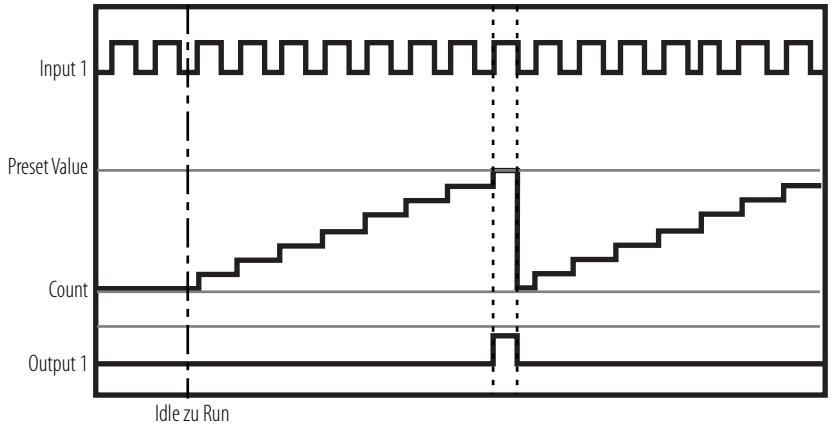
Die Zählung kann wahlweise auf Abwärtszählung (abnehmend) oder Aufwärtszählung (zunehmend) eingestellt werden.

Bei der Abwärtszählung wird der Sollwert als Anfangswert für den Zähler verwendet, und der Zähler wird mit jedem registrierten Eingangsimpuls um eins verringert. Das Signal „Output Enable“ (Ausgangsaktivierung) wird eingeschaltet, sobald die Zählung den Wert Null (0) erreicht. Der Sollwert für den Zähler wird im internen Arbeitsbereich des Zählers gespeichert und kann mit einem Programmiergerät überwacht werden.

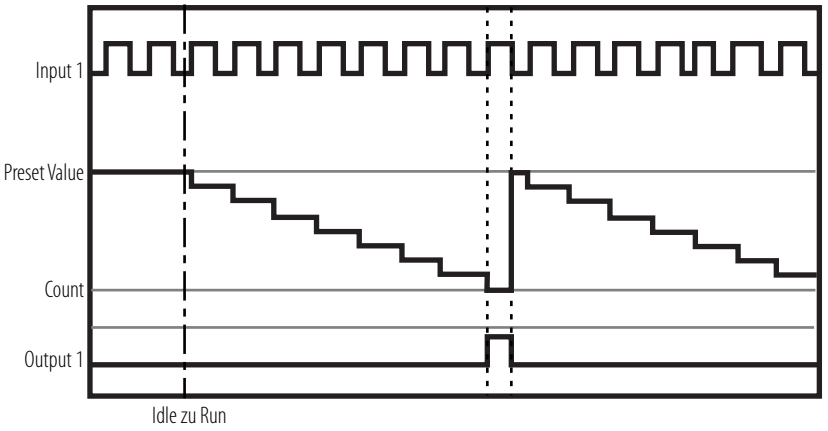
Bei der Aufwärtszählung ist der Anfangswert des Zählers Null (0), und der Zähler wird mit jedem registrierten Eingangsimpuls um eins erhöht. Das Signal „Output Enable“ wird eingeschaltet, sobald der Zähler den Sollwert erreicht.

Zeitdiagramme für den Funktionsblock Counter

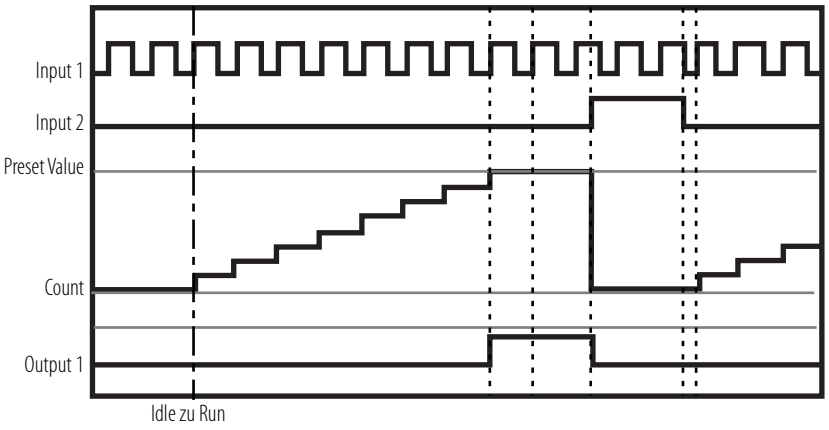
Automatische Rücksetzung – Aufwärtszählung



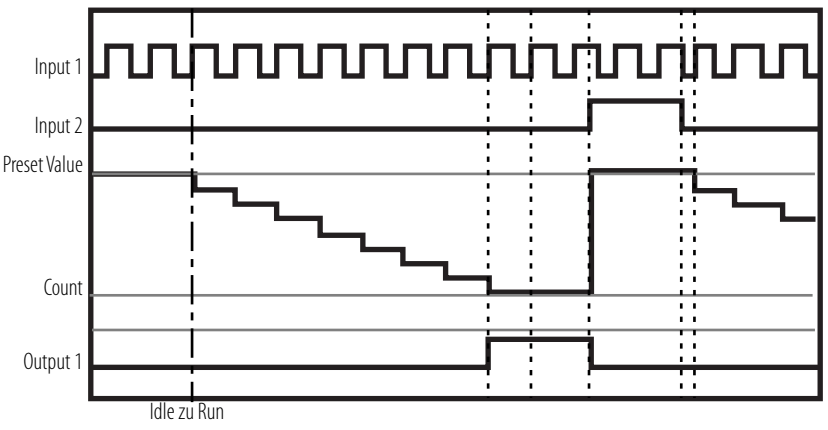
Automatische Rücksetzung – Abwärtszählung



Manuelle Rücksetzung – Aufwärtszählung



Manuelle Rücksetzung – Abwärtszählung



Notizen:

Explizite Nachrichten

Einleitung

Thema	Seite
Empfangen expliziter Nachrichten	281
Senden expliziter Nachrichten	284
Zugriff auf Steuerungsparameter mit expliziten DeviceNet-Nachrichten	286

Empfangen expliziter Nachrichten

Durch Senden einer expliziten Nachricht von einem Standard-DeviceNet-Master zur SmartGuard-Steuerung können beliebige Daten oder Parameter der SmartGuard-Steuerung gelesen oder geschrieben werden. Die Steuerung reagiert auf einen vom Master gesendeten Befehl und gibt eine entsprechende Antwort zurück.

Mit einem Lesebefehl wird der zentrale SmartGuard-E/A-Bereich oder der Sicherheits-Slave-E/A-Bereich gelesen, der der SmartGuard-Steuerung vom Master zugewiesen wurde.

Das grundlegende Format des Befehls und der Antwort wird im Folgenden erläutert.

Befehlsformat

Zielnetzknoten-adresse	Dienstcode	Klassen-ID		Instanz-ID		Offsetadresse		Daten-größe	
	4B	03	56						

Normales Antwortformat

Anzahl der Empfangsbytes	Ursprungsnetzknoten-adresse	Dienst-code	Gelesene Daten						
		CB							

Fehlerantwortformat

Anzahl der Empfangsbytes		Ursprungsnetzknoten-adresse	Dienst-code	Fehlercode	
00	04		94		

Befehlsformat

Die Zielnetzknotenadresse (Destination Node Address) gibt, in 1 Byte hexadezimal, die Netzknotenadresse der Daten an, die gelesen werden sollen.

Geben Sie bei Befehlen „4B“ (hexadezimal) als Dienstcode (Service Code) an.

Die Klassen-ID (Class ID) für eine SmartGuard-Steuerung lautet immer 0356.

Die Instanz-ID (Instance ID) ist abhängig vom Nachrichtentyp.

Instanz-ID-Werte

Expliziter Nachrichtentyp	Dienst	Instanz-ID
Zentralen Eingangsbereich lesen	Lesen	0001 (hex)
Zentralen Ausgangsbereich lesen	Lesen	0002 (hex)
Entfernten Sicherheitseingangsbereich lesen	Lesen	0005 (hex)
Entfernten Sicherheitsausgangsbereich lesen	Lesen	0006 (hex)

Die Befehlsdaten enthalten die Offset- und die Datengröße. Die Offsetgröße gibt die Adresse an, ab der gelesen werden soll. Der Offset wird in Byte beginnend bei der ersten Zeile des Bereichs angegeben. Die Datengröße gibt die Anzahl der zu lesenden Bytes 1...256 an. Im Folgenden werden die Bereichswerte zum Ermitteln des Offsets und der Größe für die verschiedenen Datenbereiche aufgeführt.

Bereichswerte

Bereich	Bereich
Zentraler Eingangsbereich	0 oder 1
Zentraler Ausgangs-/Testausgangsbereich	0 oder 1
Entfernter Sicherheitseingangsbereich	0 bis 551
Entfernter Sicherheitsausgangsbereich	0 bis 551

Antwortformat

Die Anzahl der Empfangsbytes (Number of Receive Bytes) in einer Antwort zeigt die Anzahl der Empfangsdatenbytes von der Netzknotenadresse bis zum Ende der Rückantwort an (im Hexadezimalformat).

Der Ursprungsnetzknoten (Originating Node) einer Antwort gibt die Netzknotenadresse der antwortenden SmartGuard-Steuerung als 1 Byte hexadezimal zurück.

Bei Antworten ist das obere Bit eingeschaltet, und es wird CB (hexadezimal) als Dienstcode zurückgegeben.

Die gelesenen Daten (Read Data) in einer Antwort enthalten die aus dem angegebenen Bereich zurückgegebenen E/A-Daten. Die Adressoffsets und Bitzuweisungen für das Lesen von zentralen Eingängen und Ausgängen sowie von Testausgängen sind im Folgenden aufgeführt. Bei diesen Bits entspricht 1 einem normalen und 0 einem Fehlerzustand.

Zentrale Eingänge (2 Byte)

Offset (in Byte)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Sicherheitseingangsklemme Nummer 7	Sicherheitseingangsklemme Nummer 6	Sicherheitseingangsklemme Nummer 5	Sicherheitseingangsklemme Nummer 4	Sicherheitseingangsklemme Nummer 3	Sicherheitseingangsklemme Nummer 2	Sicherheitseingangsklemme Nummer 1	Sicherheitseingangsklemme Nummer 0
1	Sicherheitseingangsklemme Nummer 15	Sicherheitseingangsklemme Nummer 14	Sicherheitseingangsklemme Nummer 13	Sicherheitseingangsklemme Nummer 12	Sicherheitseingangsklemme Nummer 11	Sicherheitseingangsklemme Nummer 10	Sicherheitseingangsklemme Nummer 9	Sicherheitseingangsklemme Nummer 8

Zentrale Ausgänge und Testausgänge (2 Byte)

Offset (in Byte)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Sicherheitsausgangsklemme Nummer 7	Sicherheitsausgangsklemme Nummer 6	Sicherheitsausgangsklemme Nummer 5	Sicherheitsausgangsklemme Nummer 4	Sicherheitsausgangsklemme Nummer 3	Sicherheitsausgangsklemme Nummer 2	Sicherheitsausgangsklemme Nummer 1	Sicherheitsausgangsklemme Nummer 0
1	Reserviert				Testausgangsklemme Nummer 3	Testausgangsklemme Nummer 2	Testausgangsklemme Nummer 1	Testausgangsklemme Nummer 0

Fehlerantwortformat

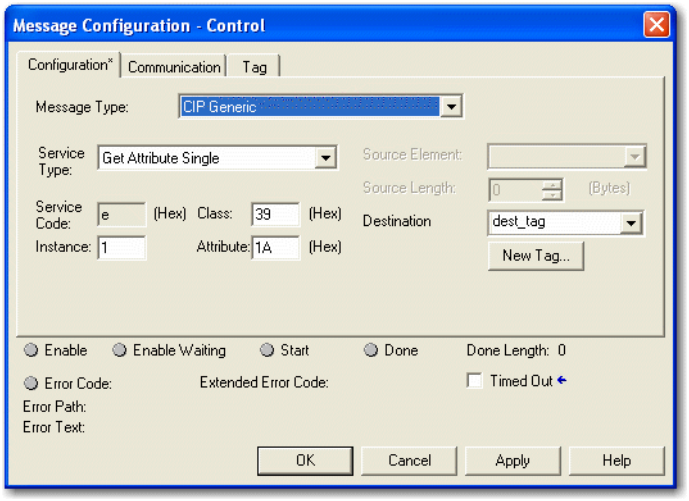
Wie bei normalen Antworten enthält eine Fehlerantwort die Anzahl der Empfangsbytes, die Ursprungsnetzknotenadresse und den Dienstcode. Außerdem enthalten Fehlerantworten einen DeviceNet-Fehlercode.

DeviceNet-Fehlercodes für explizite Nachrichten

Antwortcode	Fehlername	Beschreibung
08FF	Service not supported (Dienst wird nicht unterstützt)	Der Dienstcode enthält einen Fehler.
16FF	Object does not exist (Objekt existiert nicht)	Die angegebene Instanz-ID wird nicht unterstützt.
15FF	Too much data (Datenmenge zu groß)	Die Anzahl der Daten übersteigt die angegebene Größe.
13FF	Not enough data (Zu wenig Daten)	Die Anzahl der Daten unterschreitet die angegebene Größe.
20FF	Invalid parameter (Ungültiger Parameter)	Die angegebenen Befehlsdaten werden nicht unterstützt.

Beispiel für eine Lesenachricht einer GuardLogix-Steuerung

Dieser GuardLogix-Nachrichtenbefehl, der in der Software RSLogix 5000 mit den Befehlsformatparametern von Seite 281 programmiert wurde, liest die SmartGuard-Daten.



Senden expliziter Nachrichten

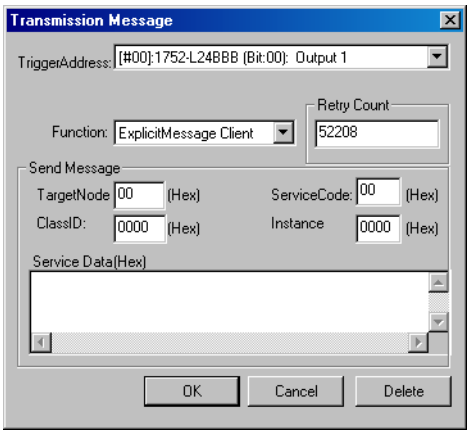
Eine SmartGuard-Steuerung kann explizite Nachrichten aus einem Anwenderprogramm senden. Vom Anwender registrierte Nachrichten werden über das Netzwerk gesendet, sobald die vom Anwender angegebenen Auslösebedingungen erfüllt sind. Dieses Verfahren kann zur Benachrichtigung von Überwachungs- und Steuergeräten oder zum Festlegen von Ausgaben an Anzeigegeräte verwendet werden. Es können bis zu 32 Datenbytes in einer expliziten Nachricht gesendet werden.

Datenformat für explizite Nachrichten

Parametername	Datengröße
MAC ID (MAC-ID)	1 Byte
Dienstcode	1 Byte
Klassen-ID	2 Byte
Instanz-ID	2 Byte
Service Data (Dienstdaten)	0 bis 26 Byte

Folgen Sie diesen Anweisungen, um mit dem Logik-Editor in der Software RSNetWorx for DeviceNet eine explizite Nachricht zu senden.

1. Wählen Sie auf der Menüleiste „Function“ > „Transmission Message Setting“ (Funktion > Einstellung Nachrichtenübertragung).



2. Wählen Sie im Pulldown-Menü „TriggerAddress“ (Auslöseadresse) das Ausgangs-Tag aus, das Sie als Auslöser für das Senden der expliziten Nachricht verwenden möchten.

   Jedes Mal, wenn das angegebene Ausgangs-Tag von aus nach ein wechselt, wird die festgelegte explizite Nachricht gesendet.

3. Geben Sie im Feld „Retry Count“ (Zahl der Neuversuche) die Zahl der Sendeversuche beim Fehlschlagen einer Übertragung ein.

   Geben Sie 0 ein, wenn die Nachricht bei einem Fehler nicht erneut gesendet werden soll.

4. Überprüfen Sie das explizite Nachrichtenformat des Zielnetzknotens, und erstellen Sie eine Sendenachricht basierend auf der Spezifikation für den Zielnetzknoten unter Angabe von „TargetNode“, „ServiceCode“, „Class ID“ und „Instance ID“.

Einschränkungen beim Senden expliziter Nachrichten

Explizite Nachrichten unterliegen den folgenden Einschränkungen.

- Im Anwenderprogramm kann eine Adresse als Auslöseadresse angegeben werden.
- Der interne E/A-Speicher der SmartGuard-Steuerung wird als Antwort auf eine explizite Nachricht gesendet. Explizite Nachrichten können von einem Anwenderprogramm in der Steuerung gesendet werden, interne Informationen der Steuerung können jedoch nicht als Daten in die gesendete Nachricht aufgenommen werden.

- Die Antwortdaten für eine explizite Nachricht können im Anwenderprogramm einer SmartGuard-Steuerung nicht verwendet werden.

ACHTUNG

Die bei der Kommunikation über Standard-E/A und explizite Nachrichten verwendeten Datenattribute werden nicht sicher gesendet. Es werden keine der für Sicherheitsdaten erforderlichen Maßnahmen durchgeführt, wenn Daten für Standardübertragungen oder explizite Nachrichten erstellt werden. Verwenden Sie diese Daten nicht für den Betrieb eines Sicherheitssteuerungssystems.

Zugriff auf Steuerungsparameter mit expliziten DeviceNet-Nachrichten

Sie können Steuerungsparameter lesen und schreiben, indem Sie explizite DeviceNet-Nachrichten an die SmartGuard-Steuerung senden. Die Steuerung verarbeitet die empfangenen Nachrichten und gibt eine Antwort zurück. Die in den folgenden Tabellen beschriebenen Nachrichten werden von der SmartGuard-Steuerung unterstützt.

Lesen des allgemeinen Status

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienstcode	Klassen-ID Hex	Instanz-ID Hex	Attribut-ID	Datengröße	
Read Unit General Status	Lesen	Liest den allgemeinen Status der Steuerung	0E hex	39 hex	01 hex	6E hex	--	1 Byte

Lesen der Sicherheitssignatur

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienstcode	Klassen-ID Hex	Instanz-ID Hex	Attribut-ID	Datengröße	
Read Unit Safety Status	Lesen	Liest die Sicherheitssignatur und den Zeitstempel der SmartGuard-Steuerung	0E hex	39 hex	01 hex	1A hex	--	10 Byte

Einstellen und Überwachen von Sicherheitseingangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienstcode	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Eingang (1…16).	0E hex	3D hex	01 bis 10 hex	65 hex	–	1 Byte 00 hex: Modus „Total On Time“ (Gesamteinschaltzeit) 01 hex: Modus „Contact Operation Counter“ (Kontaktbetriebszähler)
	Schreiben	Schreibt den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Eingang (1…16).	10 hex	3D hex	01 bis 10 hex	65 hex	1 Byte 00 hex: Modus „Total On Time“ 01 hex: Modus „Contact Operation Counter“ (Kontaktbetriebszähler)	
SV for Input Total On Time or Contact Operation Counter	Lesen	Liest den Einstellwert für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…16).	0E hex	3D hex	01 bis 10 hex	68 hex	–	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)
	Schreiben	Schreibt den Einstellwert für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…16).	10 hex	3D hex	01 bis 10 hex	68 hex	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)	–
Read Input Total On Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…16).	0E hex	3D hex	01 bis 10 hex	66 hex	–	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)
Reset Input Total On Time or Contact Operation Counter	Zurücksetzen	Setzt die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…16) zurück.	05 hex	3D hex	01 bis 10 hex	66 hex	–	–
Read Monitor Status of Input Total On Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…16).	0E hex	3D hex	01 bis 10 hex	67 hex	–	1 Byte 00 hex: im Bereich 01 hex: außerhalb des Bereichs (über dem Überwachungswert)

Einstellen und Überwachen von Sicherheitseingangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienst-code	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Read Safety Input Normal Flag	Lesen	Liest den Status des Normal-Flags mit der in der Instanz-ID angegebenen Nummer (1…16).	0E hex	3D hex	01 bis 10 hex	04 hex	–	1 Byte 00 hex: Fehler 01 hex: normal
Read Safety Input Error Information Cause	Lesen	Liest die Fehlerursache für das Normal-Flag mit der in der Instanz-ID angegebenen Nummer (1…16).	0E hex	3D hex	01 bis 10 hex	6E hex	–	1 Byte 00 hex: kein Fehler 01 hex: ungültige Konfiguration 02 hex: Testsignalfehler 03 hex: interner Schaltkreisfehler 04 hex: Diskrepanzfehler 05 hex: Fehler im anderen Kanal bei Zweikanal
Read AND of Safety Input Normal Flags	Lesen	Liest die Fehlerursache für das Normal-Flag mit der in der Instanz-ID angegebenen Nummer (1…16).	0E hex	3E hex	01 hex	05 hex	–	1 Byte 00 hex: Fehler 01 hex: alle normal
Read OR of Monitor Status of Input Total On Times or Contact Operation Counters	Lesen	Liest das Ergebnis einer logischen ODER-Verknüpfung des Überwachungsstatus für die Gesamteinschaltzeit oder die Kontaktbetriebszähler aller Eingänge 1…16.	0E hex		01 hex	72 hex	–	1 Byte 00 hex: alle im Bereich 01 hex: Eingang außerhalb des Bereichs (über dem Überwachungswert)

Einstellen und Überwachen von Sicherheitsausgangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienst-code	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Ausgang (1…8).	0E hex	3B hex	01…08 hex	65 hex	–	1 Byte 00 hex: Modus „Total On Time“ (Gesamteinschaltzeit) 01 hex: Modus „Contact Operation Counter“ (Kontaktbetriebszähler)
	Schreiben	Schreibt den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Ausgang (1…8).	10 hex	3B hex	01…08 hex	65 hex	1 Byte 00 hex: Modus „Total On Time“ (Gesamt-einschaltzeit) 01 hex: Modus „Contact Operation Counter“ (Kontakt-betriebszähler)	–
SV for Output Total On Time or Contact Operation Counter	Lesen	Liest den Einstellwert für die Gesamteinschaltzeit oder den Kontaktbe-triebszähler für den in der Instanz-ID angegebenen Eingang (1…8).	0E hex	3B hex	01…08 hex	68 hex	–	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)
	Schreiben	Schreibt den Einstellwert für die Gesamteinschalt-zeit oder den Kontaktbe-triebszähler für den in der Instanz-ID angegebenen Eingang (1…8).	10 hex	3B hex	01…08 hex	68 hex	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)	–
Read Output Total On Time or Contact Operation Counter	Lesen	Liest die Gesamtein-schaltzeit oder den Kon-taktbetriebszähler für den in der Instanz-ID angege-benen Eingang (1…8).	0E hex	3B hex	01…08 hex	66 hex	–	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)
Reset Output Total On Time or Contact Operation Counter	Zurück-setzen	Setzt die Gesamtein-schaltzeit oder den Kon-taktbetriebszähler für den in der Instanz-ID angege-benen Ausgang (1…8) zurück.	05 hex	3B hex	01…08 hex	66 hex	–	–
Read Monitor Status of Output Total On Time or Contact Operation Counter	Lesen	Liest den Überwachungs-status für die Gesamtein-schaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Ausgang (1…8).	0E hex	3B hex	01…08 hex	67 hex	–	1 Byte 00 hex: im Bereich 01 hex: außerhalb des Bereichs (über dem Überwachungswert)

Einstellen und Überwachen von Sicherheitsausgangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienst-code	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Read Safety Output Normal Flag	Lesen	Liest den Status des Normal-Flags mit der in der Instanz-ID angegebenen Nummer (1…8).	0E hex	3B hex	01…08 hex	05 hex	–	1 Byte 00 hex: Fehler 01 hex: normal
Read Safety Output Error Information Cause	Lesen	Liest die Fehlerursache für das Normal-Flag mit der in der Instanz-ID angegebenen Nummer (1…8).	0E hex	3B hex	01…08 hex	6E hex	–	1 Byte 00 hex: kein Fehler 01 hex: ungültige Konfiguration 02 hex: Überstrom registriert 03 hex: Kurzschluss registriert 04 hex: Fehler konstant hoch 05 hex: Fehler in einem der zwei Kanäle 06 hex: interner Relaisschaltkreisfehler 07 hex: Relaisfehler 08 hex: Datenfehler auf den Zweikanalausgängen 09 hex: Verdrahtungskurzschluss registriert
Read AND of Safety Output Normal Flags	Lesen	Liest die Fehlerursache für das Normal-Flag mit der in der Instanz-ID angegebenen Nummer (1…8).	0E hex	3C hex	01 hex	05 hex	–	1 Byte 00 hex: Fehler 01 hex: alle normal
Read OR of Monitor Status of Output Total On Times or Contact Operation Counters	Lesen	Liest das Ergebnis einer logischen ODER-Verknüpfung des Überwachungsstatus für die Gesamteinschaltzeit oder die Kontaktbetriebszähler aller Ausgänge 1…8.	0E hex	3C hex	01 hex	72 hex	–	1 Byte 00 hex: alle im Bereich 01 hex: Eingang außerhalb des Bereichs (über dem Überwachungswert)

Überwachen von Testausgangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienst-code	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Monitor Mode for Terminal Maintenance Information	Lesen	Liest den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Testausgang (1…4).	0E hex	35B hex	01…04 hex	83 hex	–	1 Byte 00 hex: Modus „Total On Time“ (Gesamteinschaltzeit) 01 hex: Modus „Contact Operation Counter“ (Kontaktbetriebszähler)
	Schreiben	Schreibt den Überwachungsmodus für Wartungsinformationen für den in der Instanz-ID angegebenen Testausgang (1…4).	10 hex	35B hex	01…04 hex	83 hex	1 Byte 00 hex: Modus „Total On Time“ (Gesamteinschaltzeit) 01 hex: Modus „Contact Operation Counter“ (Kontaktbetriebszähler)	–
SV for Test Output Total On Time or Contact Operation Counter	Lesen	Liest den Einstellwert für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…4).	0E hex	35B hex	01…04 hex	86 hex	–	4 Byte 0000 0000 bis FFFF FFFF hex (0 bis 4 294 967 295)
	Schreiben	Schreibt den Einstellwert für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…4).	10 hex	35B hex	01…04 hex	86 hex	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)	–
Read Test Output Total On Time or Contact Operation Counter	Lesen	Liest die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Eingang (1…4).	0E hex	35B hex	01…04 hex	84 hex	–	4 Byte 0000 0000… FFFF FFFF hex (0…4 294 967 295)
Reset Test Output Total On Time or Contact Operation Counter	Zurück-setzen	Setzt die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Testausgang (1…4) auf null zurück.	05 hex	35B hex	01…04 hex	84 hex	–	–
Read Monitor Status of Test Output Total on Time or Contact Operation Counter	Lesen	Liest den Überwachungsstatus für die Gesamteinschaltzeit oder den Kontaktbetriebszähler für den in der Instanz-ID angegebenen Testausgang (1…4).	0E hex	35B hex	01…04 hex	85 hex	–	1 Byte 00 hex: im Bereich 01 hex: außerhalb des Bereichs (über dem Überwachungswert)

Überwachen von Testausgangsklemmen

Explizite Nachricht	Dienst	Funktion	Befehl					Antwort
			Dienst-code	Klassen-ID	Instanz-ID	Attribut-ID	Datengröße	
Read Test Output Safety Flag	Lesen	Liest den Status des Normal-Flags für den in der Instanz-ID angegebenen Testausgang (1...4).	0E hex	35B hex	01...04 hex	68 hex	–	1 Byte 00 hex: normal 01 hex: Fehler
Read Test Output Error Information Cause	Lesen	Liest die Fehlerursache für das Normal-Flag des in der Instanz-ID angegebenen Testausgangs (1...4), der ausgeschaltet ist (Fehler).	0E hex	35B hex	01...04 hex	76 hex	–	1 Byte 00 hex: kein Fehler 01 hex: ungültige Konfiguration 02 hex: Überstrom registriert 05 hex: Fehler konstant hoch 06 hex: Unterstrom registriert
Read OR of Test Output Safety Flags	Lesen	Liest das Ergebnis einer logischen ODER-Verknüpfung der Normal-Flags für alle Testausgänge (1...4).	0E hex	35C hex	01 hex	69 hex	–	1 Byte 00 hex: alle normal 01 hex: Fehler
Read OR of Monitor Status of Test Output Total On Times or Contact Operation Counters	Lesen	Liest das Ergebnis einer logischen ODER-Verknüpfung des Überwachungsstatus für die Gesamteinschaltzeit oder die Kontaktbetriebszähler aller Testausgänge (1...4).	0E hex	35C hex	01 hex	72 hex	–	1 Byte 00 hex: alle im Bereich 01 hex: Testausgang außerhalb des Bereichs (über dem Überwachungswert)

Anwendungs- und Konfigurationsbeispiele

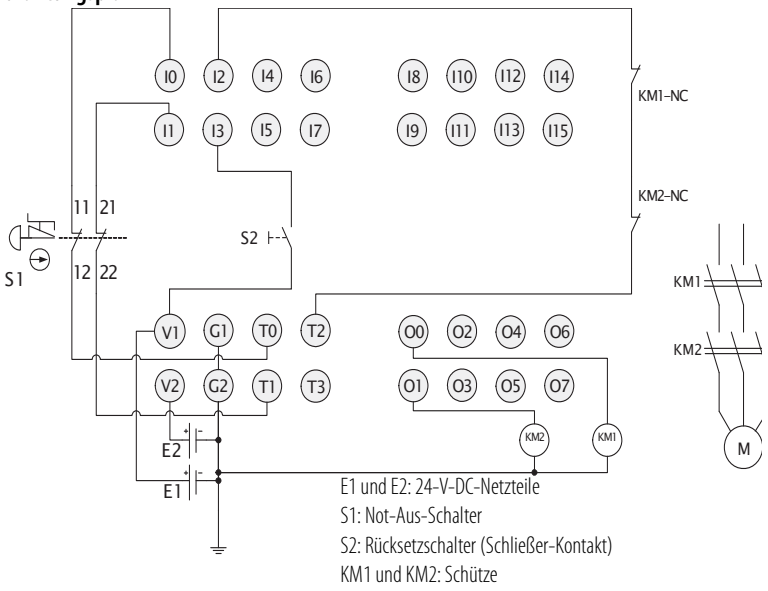
Einleitung

Thema	Seite
Not-Aus-Anwendung	293
Sicherheitstüranwendung mit automatischer Rücksetzung	295
Zwei-Zonen-Sicherheitstüranwendung unter Verwendung eines Not-Aus-Schalters mit manueller Rücksetzung	296
Sicherheitsmattenanwendung	298
Lichtgitteranwendung	300

Not-Aus-Anwendung

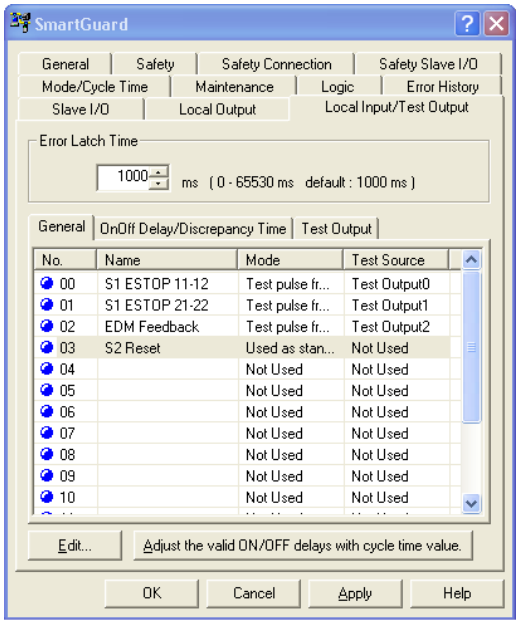
In diesem Beispiel finden Sie einen Zweikanal-Not-Aus-Schalter mit manueller Rücksetzung.

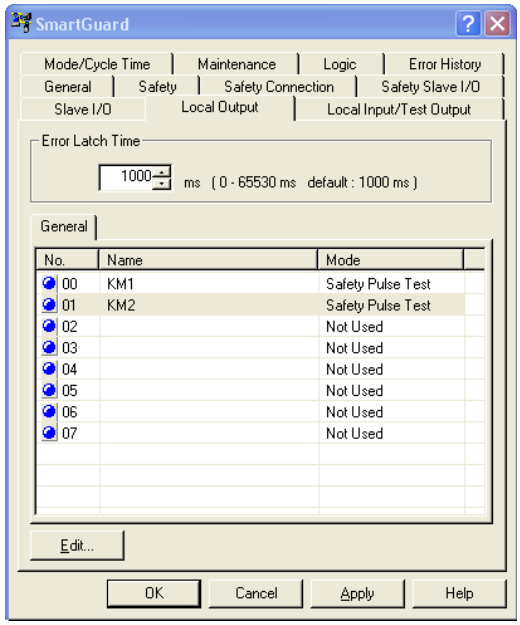
Not-Aus – Verdrahtungsplan



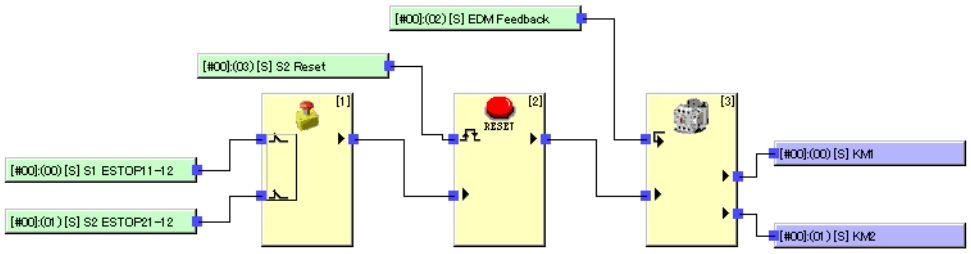
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Konfiguration

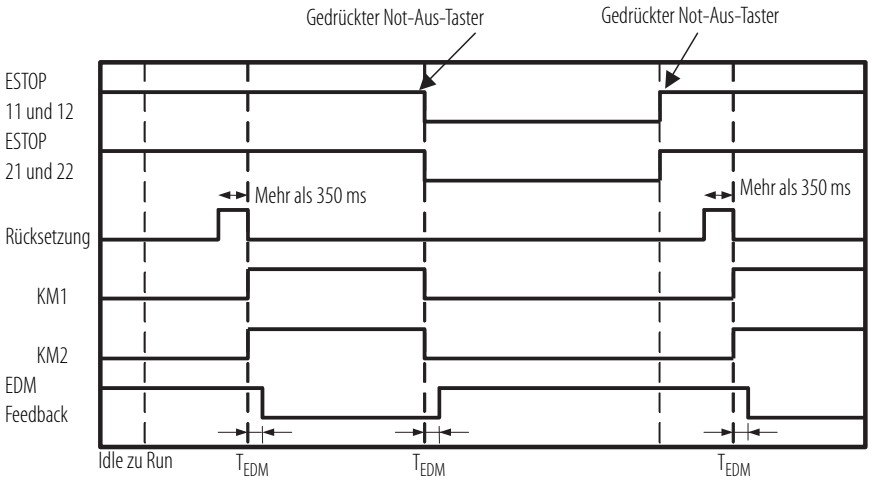




Programmierung



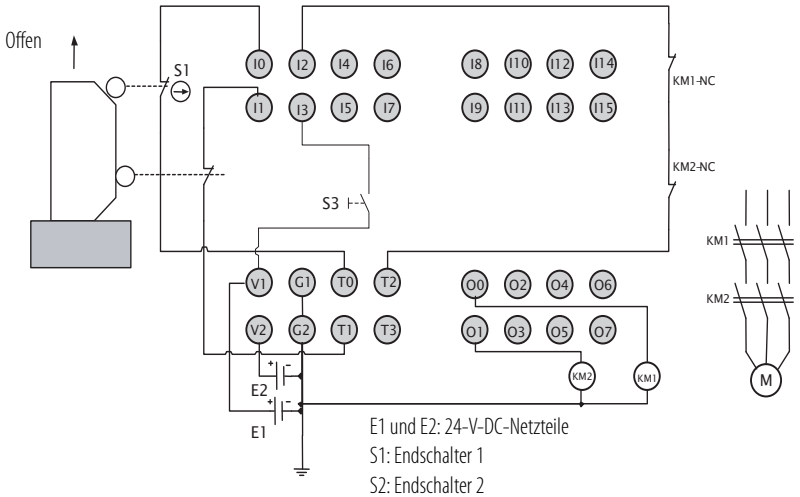
Zeitdiagramm



Sicherheitstüranwendung mit automatischer Rücksetzung

In diesem Beispiel finden Sie Zweikanal-Modus-Endschalter mit automatischer Rücksetzung.

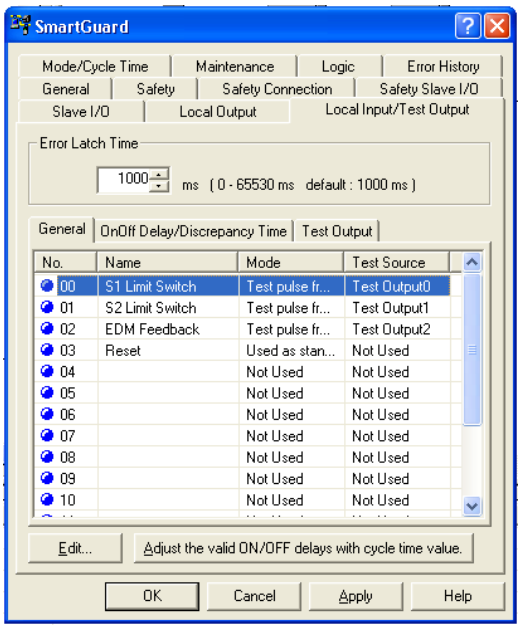
Verdrahtungsplan

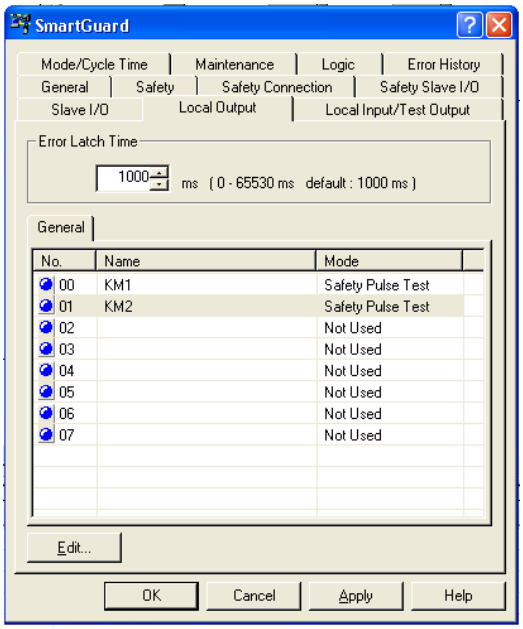


E1 und E2: 24-V-DC-Netzteile
S1: Endschalter 1
S2: Endschalter 2
S3: Rücksetzschalter
KM1 und KM2: Schütze

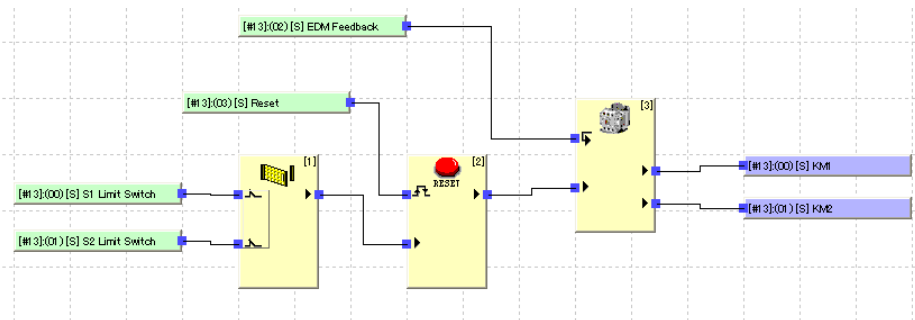
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Konfiguration

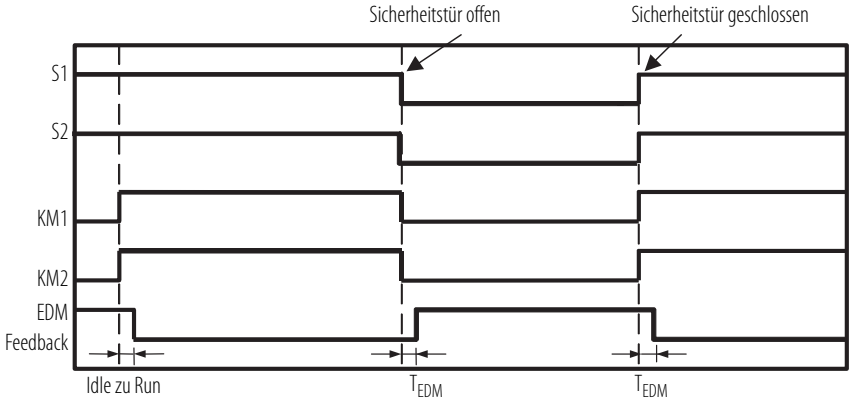




Programmierung



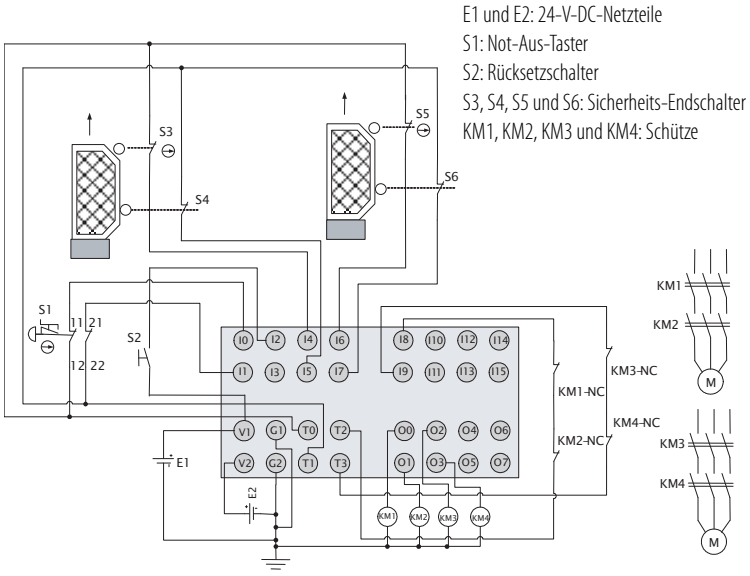
Zeitdiagramm



Zwei-Zonen-Sicherheitstüranwendung unter Verwendung eines Not-Aus-Schalters mit manueller Rücksetzung

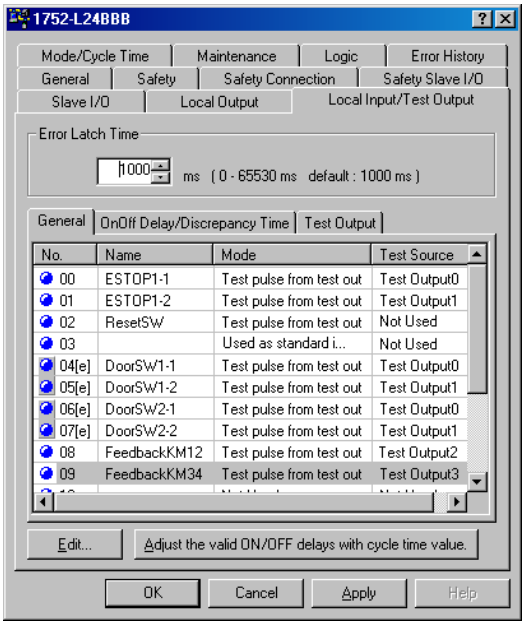
In diesem Beispiel finden Sie Zweikanal-Türschalter mit automatischer Rücksetzung und einen Zweikanal-Not-Aus-Schalter mit manueller Rücksetzung. Die einzelnen Türschalterpaare steuern jeweils eine separate Zone, sodass ein Teil der Maschine weiter ausgeführt werden kann, wenn die Tür des entsprechenden Teils geschlossen wird. Mit einem E-Stop werden beide Zonen angehalten.

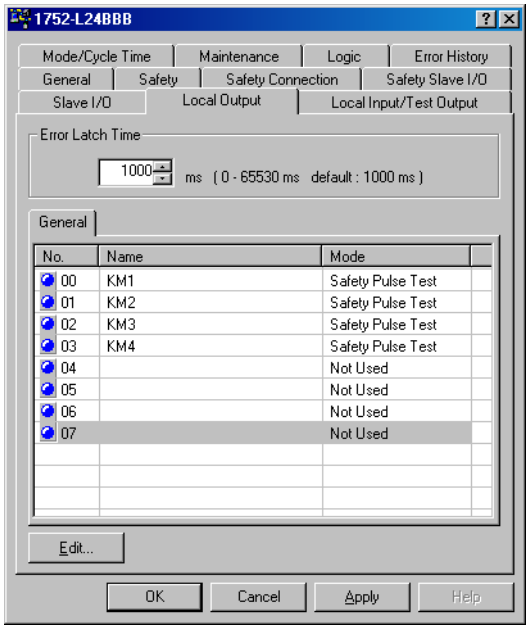
Verdrahtungsplan



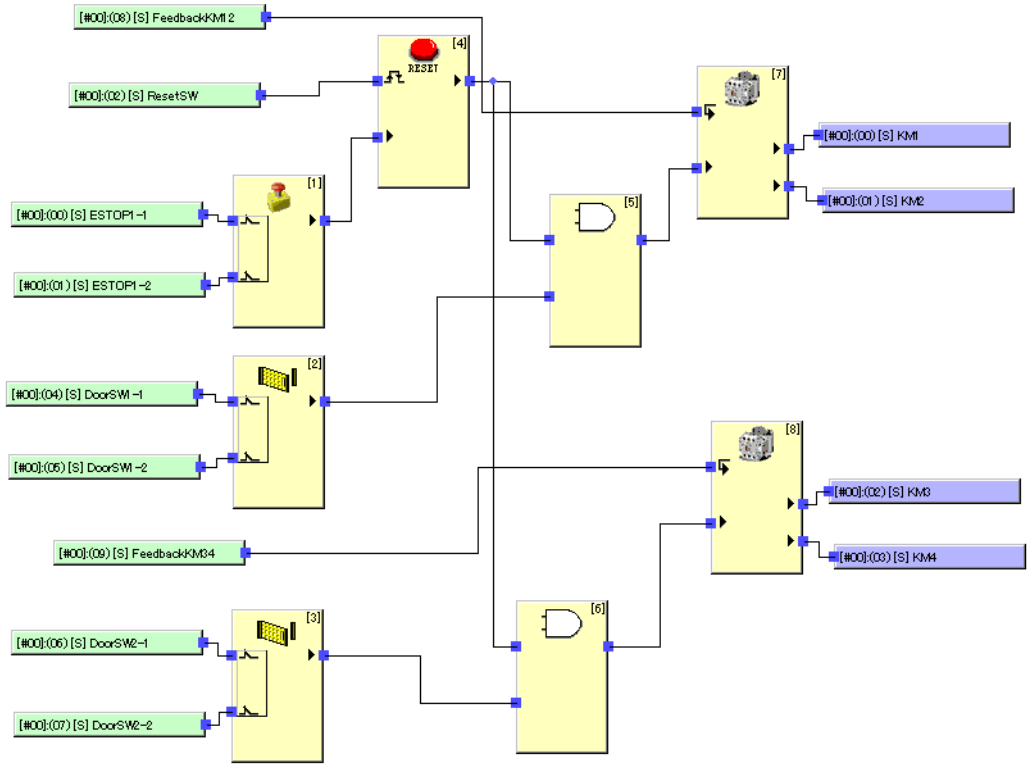
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Konfiguration

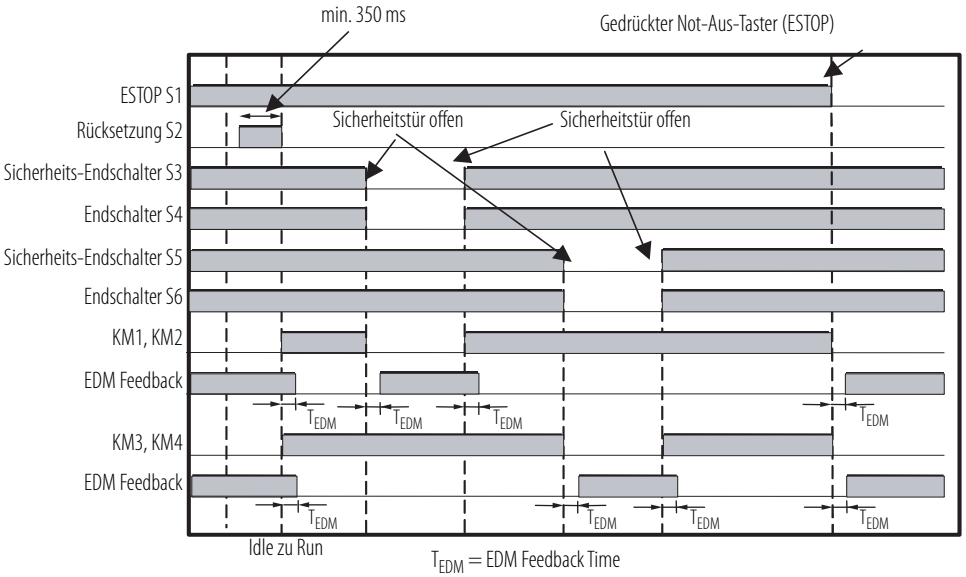




Programmierung



Zeitdiagramm

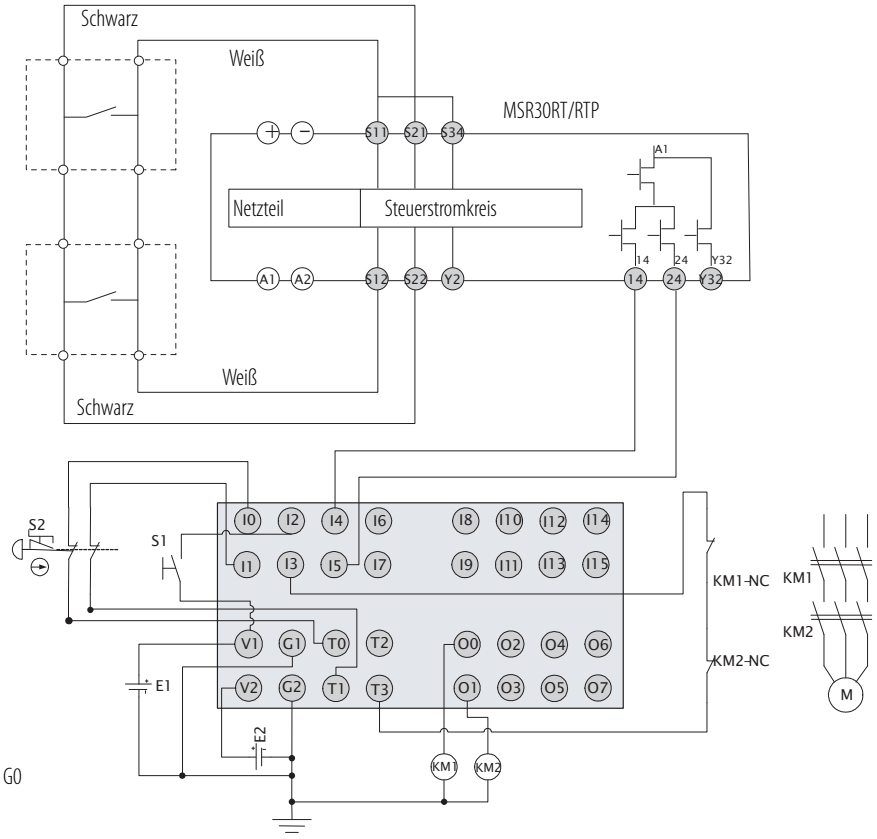


Sicherheitsmattenanwendung

In diesem Beispiel finden Sie eine Zweikanal-Sicherheitsmatte mit manueller Rücksetzung und einen Zweikanal-Not-Aus-Schalter mit manueller Rücksetzung. Für diese Anwendung wird ein MSR30RT/RTP-Relais verwendet, das über eigene Impulsaus- und -eingänge verfügt, sodass kein Testausgang der SmartGuard-Steuerung verwendet wird.

Verdrahtungsplan

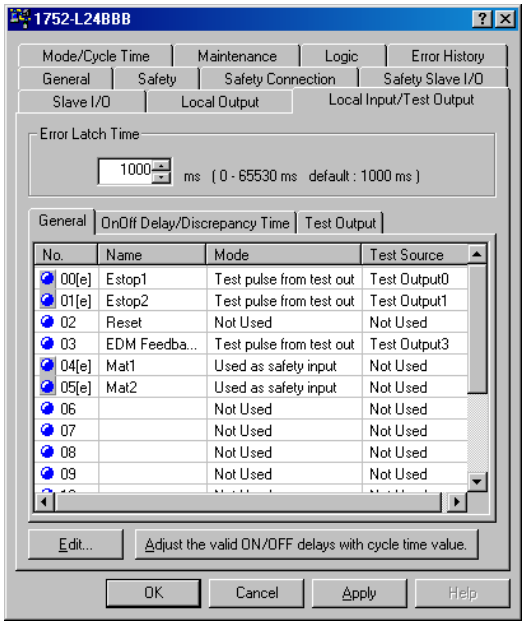
MatGuard-Matten

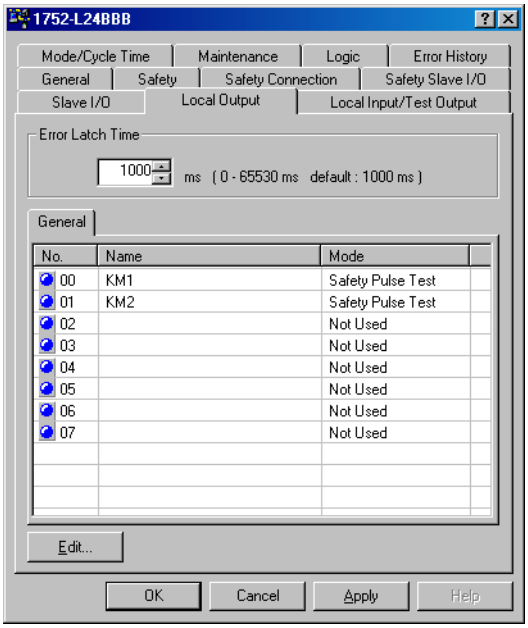


E1 und E2: 24-V-DC-Netzteile
S1: Rücksetzschalter
S2: Not-Aus-Taster
KM1 und KM2: Schütze

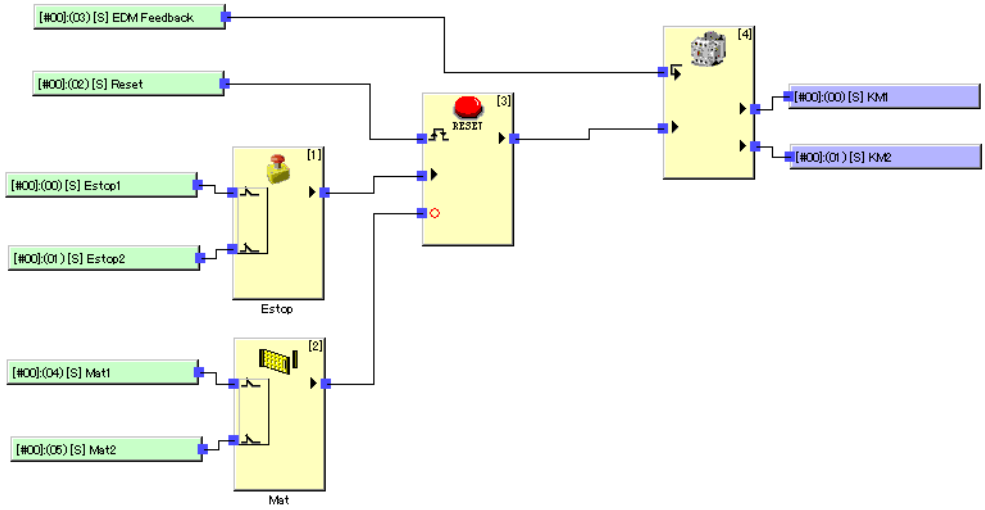
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Konfiguration

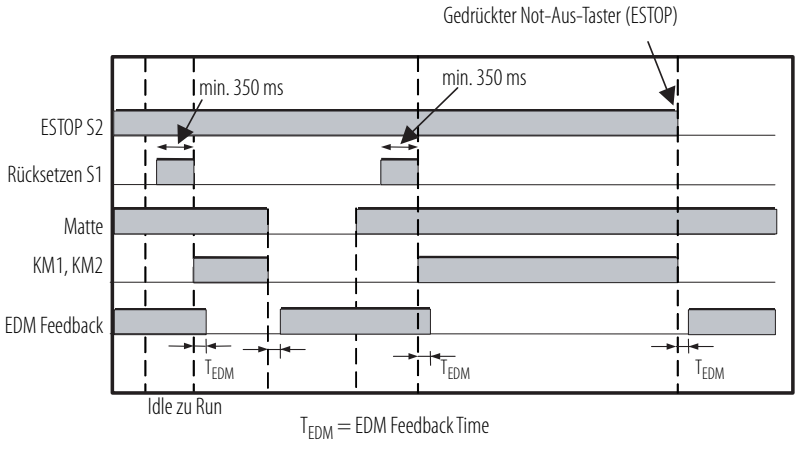




Programmierung



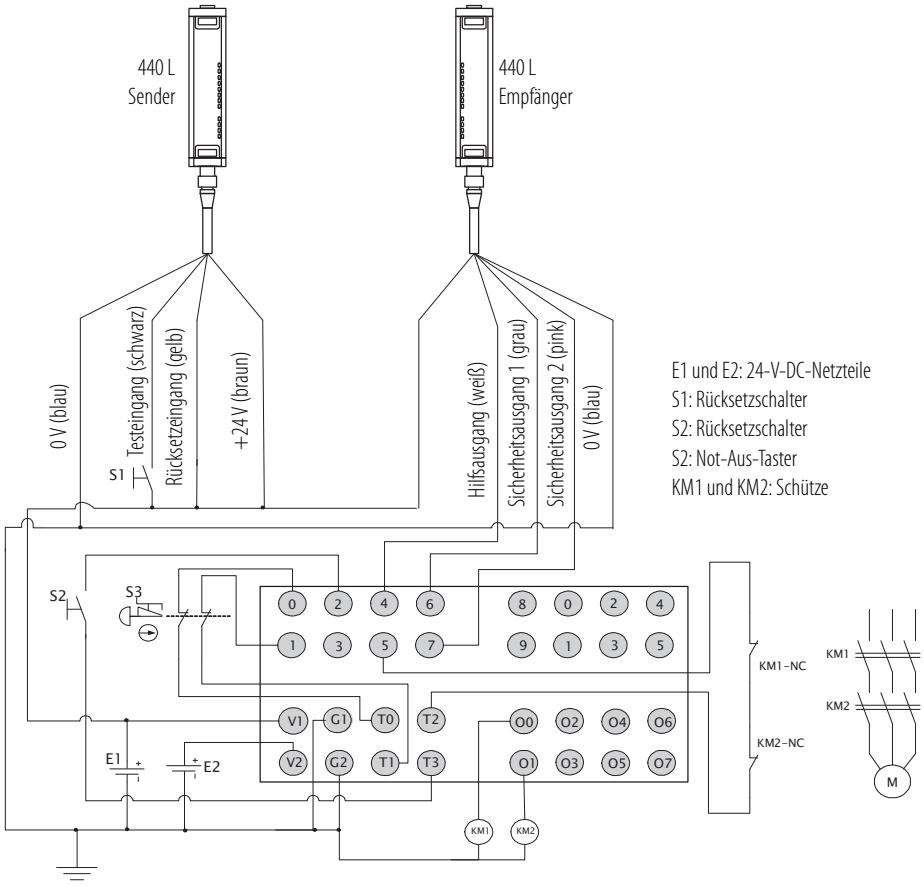
Zeitdiagramm



Lichtgitteranwendung

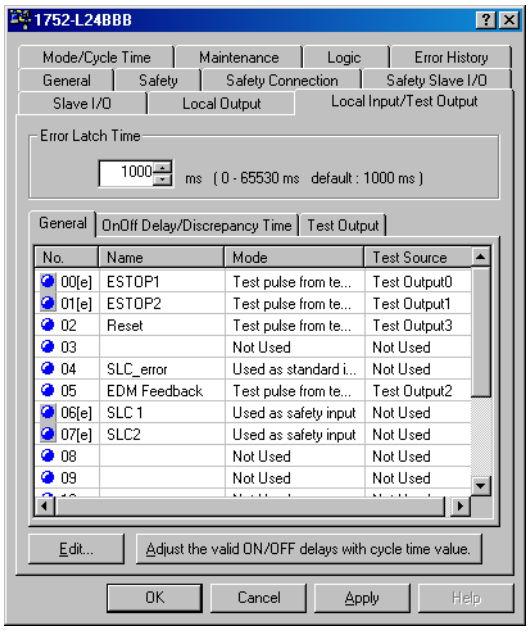
In diesem Beispiel finden Sie ein Zweikanal-Lichtgitter mit manueller Rücksetzung und einen Zweikanal-Not-Aus-Schalter mit manueller Rücksetzung.

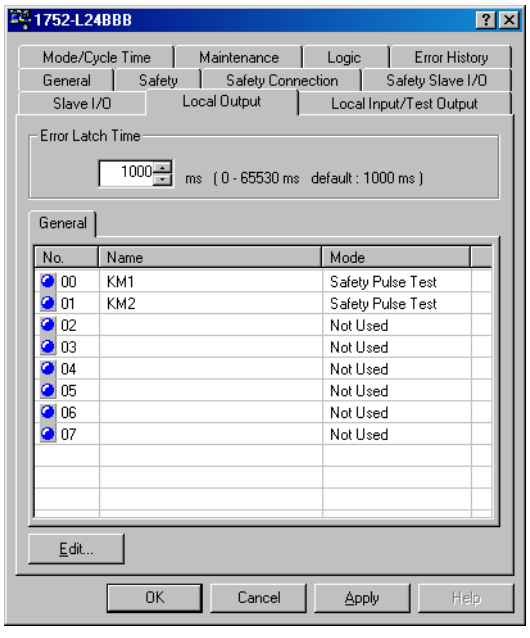
Verdrahtungsplan



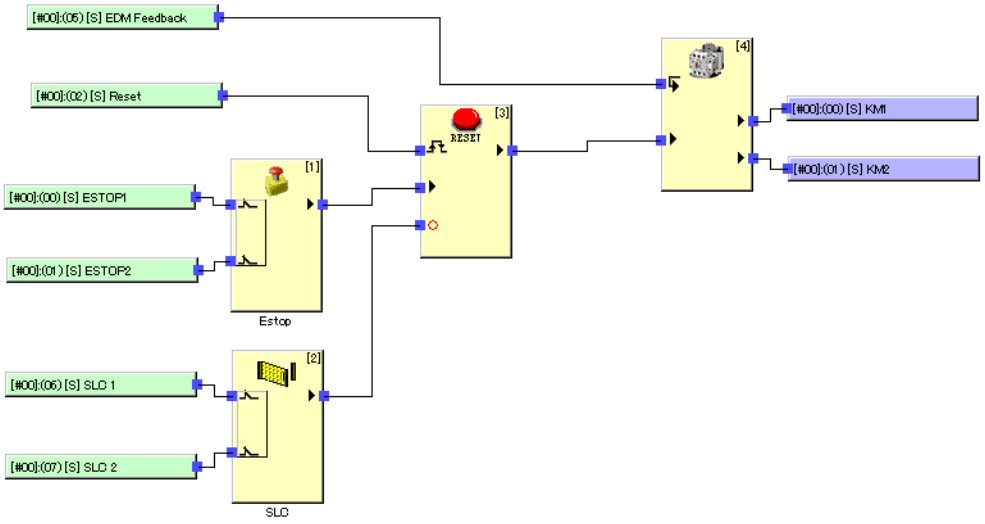
Verbinden Sie ein 24-V-DC-Netzteil mit den Klemmen V0 und G0 (Stromversorgungsklemmen für interne Schaltkreise).

Konfiguration

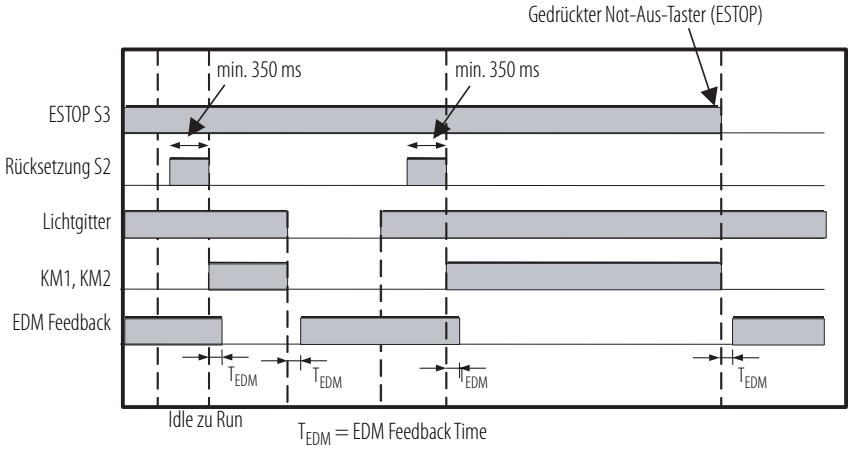




Programmierung



Zeitdiagramm



Notizen:

Abgefragt

Eine Art von Standard-E/A-Datenkommunikation, bei der eine abgefragte Nachricht eine Antwort von einem einzelnen angegebenen Gerät im Netzwerk anfordert (Punkt-zu-Punkt-Datenübertragung).

Abgetastet

Eine Art von Standard-E/A-Datenkommunikation, bei der eine Nachricht eine Antwort von jedem abgetasteten Gerät anfordert (Multicast-Übertragung). Es handelt sich um eine 64-Bit-Nachricht, die für jedes Slave-Gerät im Netzwerk ein Bit enthält.

Jeder Slave-Netzknoten kann maximal 8 Bytes als Antwort auf die Abtastung des Master-Geräts zurückgeben.

Angefordertes Paketintervall (RPI)

Bei der Kommunikation über ein Netzwerk ist das Paketintervall die erwartete Zeitspanne für die Erzeugung von Daten.

Busunterbrechung

Status, der auftritt, wenn die Fehlerrate über ein Kommunikationskabel extrem groß wird. Ein Fehler wird erkannt, wenn der interne Fehlerzähler einen Schwellenwert überschreitet.

Common Industrial Protocol (CIP)

Ein Kommunikationsprotokoll, das für industrielle Automatisierungsanwendungen konzipiert ist.

Diskrepanzzeit

Der Zeitraum zwischen dem Auftreten einer Änderung an einem von zwei Eingängen bis zum Ändern des zweiten Eingangs.

Elektronisches Datenblatt (EDS)

Eine vom Lieferanten bereitgestellte Vorlage, mit der die Software RSNetWorx for DeviceNet die Konfigurationsparameter, das E/A-Datenprofil und den unterstützten Verbindungstyp für ein bestimmtes DeviceNet- oder DeviceNet Safety-Modul anzeigen kann.

Explizite Nachrichtenübertragung

Eine Art der Nachrichtenübertragung, die für Aufgaben mit geringer Priorität verwendet wird, z. B. Konfiguration und Statusüberwachung.

Fehlerverriegelungszeit

Der Zeitraum, über den ein Fehlerzustand gehalten wird (einschließlich der zugehörigen Steuerdaten, Statusdaten und Statusanzeigen).

Gruppierung

Interne Daten in einem Gerät, die so zusammengefasst sind, dass sie von außen als eine Gruppe zugänglich sind.

Konfigurationssignatur

Die Kombination aus ID-Nummer, Datum und Uhrzeit, die eine bestimmte Konfiguration für ein Sicherheitsgerät eindeutig kennzeichnet.

Netzknoten

Hardware, der eine einzelne Adresse im Netzwerk zugewiesen wird, auch als „Gerät“ oder „Modul“ bezeichnet.

One Out of Two (1oo2) (dt.: Eins-aus-zwei-Auswertung)

Bezieht sich auf den Verhaltensentwurf eines Sicherheitssystems mit mehreren Prozessoren.

Personal-Computer (PC)

Computer, der über eine Programmiersoftware als Schnittstelle zu einem Steuerungssystem fungiert.

Probability of Failure on Demand (PFD, dt. Versagenswahrscheinlichkeit)

Die durchschnittliche Wahrscheinlichkeit, dass ein Betriebssystem seine vorgegebene Funktion auf Anforderung nicht ausführt.

Probability of Failure per Hour (PFH, dt. Wahrscheinlichkeit eines Ausfalls pro Stunde)

Die Wahrscheinlichkeit eines gefährlichen Ausfalls des Betriebssystems pro Stunde.

Sicherheits-E/A

Sicherheits-E/A weisen die meisten Attribute von Standard-E/A auf, bieten jedoch nach SIL 3 zertifizierte Mechanismen zum Prüfen der Integrität und Pünktlichkeit von Daten.

Sicherheitsnetzwerknummer (SNN – Safety Network Number)

Identifiziert ein Netzwerk eindeutig in allen Netzwerken im Sicherheitssystem. Der Endkunde muss jedem Sicherheitsnetzwerk oder Sicherheits-Teilnetz im System eine eindeutige Nummer zuweisen. Die Sicherheitsnetzwerknummer stellt einen Teil der eindeutigen Netzknoten-ID (Unique Node Identifier, UNID) dar.

Standard

Alle Objekte, Tasks, Tags, Programme oder Komponenten in Ihrem Projekt, bei denen es sich nicht um ein sicherheitsbezogenes Element handelt.

Systemreaktionszeit

Die Zeit eines sicherheitsbezogenen Ereignisses als Eingabe in das System oder als Fehler innerhalb des Systems, bis zu dem Zeitpunkt, zu dem das System sich im Sicherheitszustand befindet. Die Systemreaktionszeit umfasst Sensor- und Aktorreaktionszeiten sowie die Steuerungsreaktionszeit.

Testimpuls

Ein Signal, mit dessen Hilfe erkannt wird, wenn die externe Verdrahtung die Stromversorgung berührt (positiv) oder ein Kurzschluss zwischen Signalleitungen vorliegt.

Zustandsänderung (Change of State, COS)

Eine Art von Standard-E/A-Kommunikation, bei der die Steuerung Daten an Slave-Geräte senden und von diesen empfangen kann, wenn im konfigurierten Slave-Gerät oder in der Steuerung eine Datenänderung auftritt. Die Daten werden mit der Heartbeat-Rate aktualisiert.

Zweikanal

Die Verwendung von zwei Ein- oder Ausgängen gleichzeitig zu Redundanzzwecken.

Zweikanal-Äquivalent

Eine Einstellung zum Ermitteln, ob zwei logische Zustände äquivalent sind.

Zweikanal-Komplement

Eine Einstellung zum Ermitteln, ob zwei logische Zustände komplementär sind.

Zyklisch

Eine Art von Standard-E/A-Kommunikation, bei der die Steuerung Daten an Slave-Geräte, die zyklische Übertragungen unterstützen, senden und von diesen empfangen kann. Daten werden nur mit der benutzerdefinierten Rate gesendet.

Notizen:

A

Abweichung
- Konfigurationssignatur 168
- SNN 67

Alphanumerische Anzeige
- Fehleridentifikation 213

Angefordertes Paketintervall
- festlegen 84
- und Reaktionszeitgrenze der Verbindung 84

Assistent zur Überprüfung von Sicherheitsgeräten 47
- Ausführung 167
- Berichte 171
- Definition 167
- Geräte auswählen 169
- Gerätestatus 168
- hochladen und vergleichen 170
- Sicherheitsverriegelung
- Willkommensseite 167
- Zusammenfassung 173

Ausgangsverbindungseigentümer
- Reset 46

Ausschaltverzögerung 69

B

Baudrate
- siehe Kommunikationsgeschwindigkeit

Beispiele
- Bridging 61
- EtherNet/IP-Netzwerk zu einem DeviceNet-Netzwerk 60
- EtherNet/IP-Netzwerk zu einem USB-Anschluss 62
- RSLinx-Bridging 60, 62

Bereit zur Sicherheitsverriegelung 171

Bereit zur Überprüfung 169

BOOTP
- festlegen der IP-Adresse 54
- Verwendung des Rockwell-Dienstprogramms 55

Bridge 59

C

CIP Safety I/O
- Konfigurationssignatur 45

D

DeviceNet-Netzwerk
- konfigurieren eines Treibers 42, 52
- verbinden 41, 51

E

Eindeutige Netzknoten-ID 63

Einschaltverzögerung 69

EtherNet/IP-Modul
- Bridging 59
- Konfigurationsparameter 53

EtherNet/IP-Netzwerk
- Parameter 53
- Verbindung mit einem Computer herstellen 51

Explizite Nachricht
- Einschränkungen 285
- empfangen 281
- senden 284

F

Fehlendes Gerät
- Symbol 168

Fehlerkategorien 187

Fehlermeldungen
- Download-Fehler 196
- Kommunikation 191
- Modusänderungen 200
- Netzteil 194
- Rücksetzfehler 198
- Sicherheitsausgänge 195
- Sicherheitseingänge 195
- Systemausfall 191
- Testausgänge 195

Funktionsblock 72

G

Gateway 53

Gerätestatus
- Assistent zur Überprüfung von Sicherheitsgeräten 168
- Überprüfung 169

H

Herunterladen der DeviceNet-Konfiguration 165-166

Hochladen und vergleichen
- Assistent zur Überprüfung von Sicherheitsgeräten 170

I

Impulstestquellen 74
Inbetriebnahme der Netzknoten 42-43
  Tool 42
IP-Adresse
  festlegen mit BOOTP 54
  festlegen mit Software RSLinx 57
  Überblick 53

K

Kennwort
  festlegen oder ändern 47
  geschütze Vorgänge 47
  gültige Zeichen 48
  Reset 46, 48
  vergessen 48
Kommunikationsgeschwindigkeit
  Reset 46
Konfiguration
  DeviceNet Safety-Zielknoten 45
  Reset 46
  Sicherheitsparameter 80
  Standardparameter 82
  überprüfen 167-173
Konfigurationssignatur 45
  Abweichung 168
  Definition 45
  Komponenten 45
  Vergleich 172
Konfigurieren eines Treibers 42, 52

L

LOCK
  siehe Sicherheitsverriegelung.
Logik
  Funktionen 145

M

Multicast-Verbindungen 83
Muting-Lampe
  Statusdaten 183

N

Netzknotenadresse 43
  Änderungen 67
  auswählen 26
  Reset 46
Netzwerk
  Bridge 59
Netzwerkstatusanzeige
  blinkt 208
Netzwerkverzögerungs-Multiplikator 85

O

Online-Schaltfläche 166

P

Prüfberichte
  Assistent zur Überprüfung
    von Sicherheitsgeräten 171
  Fehlerbericht 171
Punkt-zu-Punkt 83

R

Reaktionszeitgrenze der Verbindung 84
  DeviceNet Safety I/O 84
  und Netzwerkverzögerungs-Multiplikator 85
Registerkarte „Parameters" (Parameter) 82
Registerkarte „Safety Configuration" (Sicherheitskonfiguration) 80
Registerkarte „Safety Connections" (Sicherheitsverbindungen) 83
Reset
  Konfigurationseigentümer 46
  Sicherheitsattribute 46
  Sicherheitsgerät 46, 67
Rockwell BOOTP-Dienstprogramm 55
RPI
  siehe „Angefordertes Paketintervall"
RSNetworx for DeviceNet
  Inbetriebnahme der Netzknoten 42

S

Scanner
  Reset 67
Sicherheitsnetzwerknummer 63
  Abweichung 67
  automatisch 64
  automatische Zuweisung 65
  Fehlersymbol 168
  Formate 63
  kopieren 64
  manuell 64, 65
  manuelle Zuordnung 65
  Reset 46, 67
  verwalten 63
  zeitbasiert 64
  Zuweisung 65
Sicherheits-Reset 46

Sicherheitsverriegelung
beim Zurücksetzen 47
Geräte
Symbol 168
Software RSLinx
Bridging 60, 62
konfigurieren von Netzwerkparametern 57
Software RSLogix 5000
Software, generisches Profil 134
Spezifikationen
allgemein 201
Status
anzeigen 207
Statusdaten 181
allgemein 182
Muting-Lampe 183
Testausgang 183
zentraler Ausgang 183
zentraler Eingang 183
Subnet Mask (Subnet-Maske) 53
Symbol
Gerätestatus 168

T

Testimpulsquellen
mit Eingängen 69
ohne Ausgänge 76
Timeout-Multiplikator 85
Treibertypen 42, 52

U

Überprüfen
DeviceNet-Sicherheitskonfiguration 167-173
FEHLGESCHLAGEN 171
Geräte auswählen 169
Überprüfung fehlgeschlagen 169
Überprüfung nicht unterstützt 169
Überstromerkennung
Ausgänge 76
Impulstestquellen 74
Unbekanntes Gerät
Symbol 168

W

Weiterführende Publikationen 13
Willkommensseite 167

Z

Zentral
Ausgänge 76-78
Eingänge 69-72
Zweikanalmodus
Ausgänge 77
Eingänge 69

Kundendienst von Rockwell Automation

Rockwell Automation stellt technische Informationen im Internet zur Verfügung, die Sie bei dem Einsatz unserer Produkte unterstützen. Unter http://support.rockwellautomation.com finden Sie technische Publikationen, eine Knowledge Base mit häufig gestellten Fragen (FAQs), Hinweise zu technischen Einzelheiten und zur Anwendung, Beispielcode sowie Links zu Software Service Packs und eine „MySupport"-Funktion, die Sie für eine optimale Nutzung dieser Tools anpassen können.

Für zusätzliche technische Support-Leistungen bei der Installation, Konfiguration und Fehlerbeseitigung werden TechConnect Support-Programme angeboten.
Weitere Informationen erhalten Sie bei Ihrem lokalen Distributor oder Vertreter von Rockwell Automation sowie unter http://support.rockwellautomation.com.

Unterstützung bei der Installation

Wenn innerhalb von 24 Stunden nach der Installation ein Problem auftritt, lesen Sie bitte die Informationen in diesem Handbuch. Über eine spezielle Kundendienst-Bearbeitungsnummer erhalten Sie Unterstützung beim Einrichten und Inbetriebnehmen Ihres Produkts:

USA	1.440.646.3434 Montag bis Freitag, 8.00 Uhr bis 17.00 Uhr EST
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zur technischen Unterstützung an Ihren lokalen Rockwell Automation-Vertreter.

Rückgabeverfahren bei neuen Produkten

Rockwell Automation testet alle Produkte, um sicherzustellen, dass sie beim Verlassen des Werks voll funktionsfähig sind. Sollte das Produkt dennoch nicht funktionieren und zurückgegeben werden müssen, gehen Sie wie im Folgenden beschrieben vor.

USA	Wenden Sie sich an Ihren Distributor. Sie müssen Ihrem Distributor eine Kundendienst-Bearbeitungsnummer angeben (diese erhalten Sie über die oben genannte Telefonnummer), damit das Rückgabeverfahren abgewickelt werden kann.
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zum Vorgehen bei Rückgabe an Ihren Vertreter von Rockwell Automation.

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation 1752-UM001D-DE-P – April 2009
Copyright © 2009 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in USA.